O‘ZBEKISTON RESPUBLIKASI
ICHKI ISHLAR VAZIRLIGI
MALAKA OSHIRISH INSTITUTI

KIBERJINOYATCHILIKKA QARSHI KURASHISHNING HUQUQIY, TASHKILIY, MOLIYAVIY-IQTISODIY, MUHANDISLIK-TEXNIK MUAMMOLARI VA YECHIMLARI

Respublika ilmiy-amaliy konferensiya materiallari to‘plami

Toshkent-2024
5-dekabr

O‘ZBEKISTON RESPUBLIKASI ICHKI ISHLAR VAZIRLIGI

MALAKA OSHIRISH INSTITUTI

KIBERJINOYATCHILIKKA QARSHI KURASHISHNING HUQUQIY, TASHKILIY, MOLIYAVIY-IQTISODIY, MUHANDISLIK-TEXNIK MUAMMOLARI VA YECHIMLARI

Respublika ilmiy-amaliy konferensiya materiallari to‘plami

2024-yil, 5-dekabr

Toshkent-2024

UO‘K: 343.97 (575.1)

Kiberjinoyatchilikka qarshi kurashishning huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik muammolari va yechimlari. Respublika ilmiy-amaliy konferensiya materiallari to‘plami. 2024-yil 5-dekabr. – Toshkent: O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti. 2024. - 288-bet.

To‘plam “Kiberjinoyatchilikka qarshi kurashishning huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik muammolari va yechimlari” mavzusidagi respublika ilmiy-amaliy konferensiyaning materiallari, olimlarning ilmiy maqolalari asosida tuzildi.

To‘plam professor-o‘qituvchilar, ilmiy izlanishlar olib borayotgan soha mutaxassislari, ilmiy-tadqiqotchilar, doktarantlar, magistrlar, talabalar va tinglovchilar uchun mo‘ljallangan.

Maqolalarda keltirilgan ma’lumotlarning haqqoniyligi uchun mualliflar javobgardir.

KIRISH SO‘ZI

Assalomu alaykum, Hurmatli konferensiya qatnashchilari!

XXI asr - axborot texnologiyalari asri. Qariyb chorak asr bo‘lganiga qaramasdan, dasturlash, axborotni uzatish, ma’lumotlar tahlili, axborot xavfsizligi, kiberxavfsizlik hamda sun’iy intellekt texnologiyalari sohasida o‘zgarishlar yaqqol sezilmoqda.

O‘zbekiston Respublikasi Prezidenti Shavkat Miromonovich Mirziyoyev aholiga ko‘rsatilayotgan xizmatlarni raqamlashtirishga alohida e’tibor qaratdilar. Buning natijasida 2024-yilda https://my.gov.uz/oz yagona interaktiv davlat xizmatlari portali orqali **684 ta** onlayn xizmat joriy qilindi.

Axborot texnologiyalari rivojlanib borgani sari kiberjinoyatlar salmog‘i ham o‘sib bormoqda. 2024-yil may oyida O‘zbekistonning “uz” domen veb-saytlariga **6,6 million**dan ortiq kiberhujumlar amalga oshirildi. Bu esa internet yoki ijtimoiy tarmoqlar orqali sodir etilayotgan turli huquqbuzarlik va jinoyatlarga qarshi kurashishning samarali mexanizmlarini taqozo etadi.

O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida” O‘RQ-764-son Qonunida **“kiberjinoyatchilik** — axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi” deb ta’rif berilgan.

Axborot texnologiyalari asrida jinoyatchilar bank plastik kartalaridagi pul mablag‘lari hamda fuqarolarning shaxsiy ma’lumotlarini o‘z shaxsini oshkor qilmasdan olish imkoniyatiga ega. O‘sib borayotgan kiberjinoyatlarni oldini olish, aniqlash va fosh etish uchun huquqni muhofaza qilish organlari jadal kurash olib bormoqda. 2021-2023-yillarda O‘zbekistonda kiberjinoyatlar soni **25 baravar**ga oshgani, soha mutaxassislaridan yuqori malakani talab qiladi.

O‘zbekiston Respublikasi Prezidentining 2023-yil 30-noyabrdagi “Raqamli mahsulotlar (xizmatlar) iste’molchilari huquqlarini himoya qilish va raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarga qarshi kurashishni kuchaytirish choralari to‘g‘risida” PQ-381-son qaroriga asosan, soha mutaxassislari kiberjinoyatchilikka qarshi kurashishda o‘z malakalarini oshirib borishi yo‘lga qo‘yildi.

O‘zbekiston Respublikasi Ichki ishlar vazirligida kiberxavfsizlikni ta’minlash, kiberjinoyatlarni oldini olish, aniqlash va fosh etish Axborot texnologiyalari aloqa va axborotni himoyalash boshqarmasi, Tezkor qidiruv departamenti Kiberxavfsizlik markazi hamda Ekspert kriminalistika bosh markazining Raqamli axborot-qidiruv tizimlari markazi mas’ul xodimlari tomonidan amalga oshirib kelinmoqda.

Yuqoridagi me’yoriy-hujjatlarda belgilangan vazifalarni amalga oshirish maqsadida, O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish institutida 2024-yil 5-dekabr kuni “Kiberjinoyatchilikka qarshi kurashishning huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik muammolari va yechimlari” mavzusidagi respublika ilmiy-amaliy konferensiya o‘tkazilmoqda.

Hurmatli konferensiya ishtirokchilari!

Umid qilamanki, bugun o‘tkazilayotgan respublika ilmiy-amaliy konferensiyada ko‘rib chiqiladigan muammolar, bildiriladigan fikrlar, takliflar va tavsiyalar yurtimizda kiberjinoyatlarni oldini olish, aniqlash va fosh etishda ko‘mak bo‘ladi.

So‘zim yakunida menga berilgan vakolatdan foydalanib, konferensiyani ochiq deb e’lon qilaman hamda barcha ishtirokchilarga muvaffaqiyatlar tilayman!

E’tiboringiz uchun rahmat.

O.T. Axmedov

O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti boshlig‘i, t.f.n, dotsent

ICHKI ISHLAR ORGANLARI XODIMLARINI TAYYORLASHDA SUN'IY INTELLEKTNING O'RNI

Ulug'bek Erkinovich Rasulev

O'zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti boshlig'ining birinchi o'rinbosari

Ilm-fan, texnologiya va kommunikatsiyalarning jadal rivojlanishi bilan ajralib turadigan zamonaviy dunyoda rivojlangan mamlakatlar sun'iy intellektni davlat boshqaruvi, iqtisodiyot, sanoat, ijtimoiy himoya, ta'lim, sog'liqni saqlash, bandlik, qishloq xo'jaligi, mudofaa, xavfsizlik va turizm kabi turli sohalarga faol joriy etmoqda.

Sun'iy intellekt hayotimizga tobora chuqurroq kirib bormoqda va tabiiy ravishda "Bu nima o'zi?" degan savol tug'iladi. Sun'iy intellektga ta'rif berishdan oldin "intellekt" tushunchasini anglash lozim. Intellekt - bu insonning atrofidagi dunyoni bilish va o'zgartirish, fikrlash, o'rganish, bilim va ijtimoiy tajribani to'plash qobiliyati, qaror qabul qilish, oqilona harakat qilish, voqealarni oldindan ko'ra bilish layoqatidir.

Intellekt idrok etish, eslab qolish, fikrlash va boshqa psixologik jarayonlarni o'z ichiga oladi. Ushbu ta'rifdan kelib chiqadiki, intellekt faqat insonga xos bo'lib, uning aqliy qobiliyatlarining mezonini tashkil etadi.

Bugungi kunda sun'iy intellektning yagona, umum e'tirof etilgan ta'rifi mavjud emas. Bu turli soha olimlarining ushbu tushunchani har xil talqin qilishlari bilan izohlanadi. "Sun'iy intellekt" atamasining muallifi Jon Makkarti bir nechta ta'riflarni taklif etgan. U sun'iy intellektni "intellektual mashinalarni, ayniqsa, intellektual kompyuter dasturlarini yaratish ilmi va muhandislik san'ati" deb ta'riflagan[1]. Sun'iy intellekt bo'yicha ko'plab ilmiy ishlar muallifi, taniqli olim Nils Nilson esa uni "tabiiy intellektga taqlid qiluvchi sun'iy aql yaratishga qaratilgan nazariya" deb ta'riflagan[2].

Shunday qilib, sun'iy intellekt - bu olingan ma'lumotlardan foydalanib, asta-sekin o'zini takomillashtirgan holda, ma'lum vazifalarni bajarishda insonning harakatlarini imitatsiya qila oladigan tizim yoki texnologiyadir. Shuni tushunish kerakki, sun'iy intellekt - bu format yoki funksiya emas, balki ma'lumotlarni to'plash va tahlil qilishni o'z ichiga olgan jarayondir.

Ko'pincha odamlar sun'iy intellektni turli vazifalarni bajaruvchi robotlar bilan bog'laydilar. Biroq sun'iy intellektni joriy etish insonni robotlar bilan almashtirishni anglatmaydi. Sun'iy intellektning asosiy maqsadi insonning imkoniyatlari va salohiyatini kengaytirishdir. Shuning uchun ham bunday texnologiyalar qimmatli biznes resursi hisoblanadi.

O'zbekistonda sun'iy intellektni joriy etish va rivojlantirish bo'yicha bir qator chora-tadbirlar qabul qilingan. O'zbekiston Respublikasi Prezidentining 2021-yil 17-fevraldagi "Sun'iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to'g'risida"gi qaroriga (PQ-4996) muvofiq sun'iy intellektning yangi texnologiyalarini soddalashtirilgan tartibda joriy etish mamlakatimiz qonunchiligida mustahkamlab qo'yilgan. "Raqamli O'zbekiston –

[1] Маккарти Дж. Эпистемологические проблемы искуственного интелекта. 1977. – С.21.

2 https://en.wikipedia.org/wiki/Nils John Nilsson

2030” strategiyasi doirasida mamlakatda sun’iy intellektni keng qo‘llash, raqamli ma’lumotlarning mavjudligi va sifatini ta’minlash, shuningdek, ushbu sohada malakali kadrlar tayyorlash uchun qulay shart-sharoitlar yaratish maqsad qilingan.

Ichki ishlar organlarida ham sun’iy intellektni joriy etish bo‘yicha faol ishlar olib borilmoqda. Masalan, yo‘l harakati xavfsizligini ta’minlash sohasida “Avtomototransport vositalari to‘g‘risida ma’lumot” va “Yo‘l-transport hodisalari to‘g‘risida ma’lumot” ma’lumotlar bazalari hamda qidiruvdagi shaxslarni aniqlash uchun dasturiy ta’minot yaratilgan.

Sun’iy intellektni ichki ishlar tizimiga, ayniqsa, ta’lim tizimiga joriy etish sezilarli natijalarga olib kelishi mumkin. Sun’iy intellekt shaxsga yo‘naltirilgan o‘qitish tizimlarida, ma’lumotlarni izlashda, chat-botlarda, inklyuziv o‘qitish tizimlarida, o‘quv jarayonini nazorat qilish tizimlarida va o‘quvchilar bilimini baholash tizimlarida qo‘llanilishi mumkin. Bunday tizimlardan foydalanish o‘qituvchilarning malakasini oshirishga va ularning ish yukini kamaytirishga yordam beradi.

Sun’iy intellekt yordamida zamonaviy ta’limni tashkil etishning asosiy talablaridan biri ortiqcha aqliy va jismoniy zo‘riqishlarsiz qisqa vaqt ichida yuqori natijalarga erishishdir. Sun’iy intellekt ma’lum nazariy bilimlarni cheklangan vaqt ichida yetkazib berish va o‘quvchilarda ma’lum harakatlarni bajarish uchun ko‘nikma va malakalarni shakllantirish imkonini beradi. Bu IIV Malaka oshirish institutida xodimlarning egallagan bilim, ko‘nikma va malakalari darajasi ular topshirgan imtihonlar natijalariga ko‘ra baholanadigan xizmatning tegishli yo‘nalishlari bo‘yicha masofaviy o‘qitish uchun dolzarbdir.

Ta’lim jarayoniga sun’iy intellektni joriy etish o‘qituvchilardan ham o‘zgarishlarni talab qiladi. Ishlab chiqilgan dasturlar o‘quvchilarning yanada tezroq, samarali va sifatli ta’lim olishiga ko‘maklashadi. Bu esa o‘z navbatida o‘qituvchilarni o‘zlarini takomillashtirishga va o‘qitish sifatini oshirishga undaydi.

Xulosa qilib aytganda, ta’limga sun’iy intellektni joriy etish o‘qituvchilarning ko‘plab vazifalarini optimallashtirish va avtomatlashtirish imkonini beradi, ularning o‘quvchilar bilan ishlash va ta’lim sifatini oshirish uchun vaqtini bo‘shatadi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Prezidentning 2021 yil 17 fevraldagi «Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to‘g‘risida»gi PQ-4996-son Qarori.
2. Makkarti Dj. Epistemologicheskie problemы iskustvennogo intelekta. 1977. – S.21.
3. https://uz.wikipedia.org/wiki/intelekt.
4. https://en.wikipedia.org/wiki/Nils John Nilsson.

ОНЛАЙН САВДО ПЛАТФОРМАЛАРИ ОРҚАЛИ СОДИР ЭТИЛАЁТГАН КИБЕРЖИНОЯТЛАРНИ ФОШ ЭТИШГА КЎМАКЛАШУВЧИ ТИЗИМЛАР

Садиков Саидкамол

ИИВ ТҚД Киберхавфсизлик маркази, PhD

Бугунги кунда бутун дунё бўйлаб кенг фойдаланиб келинаётган онлайн савдо платформалари маҳсулотлар харидини амалга оширишда инқилобий ўзгаришларни юзага келтирди. Мазкур платформалар харидор/истеъмолчига ҳам сотувчи/хизмат кўрсатувчига ҳам бир қатор қулайликлар яратиши омилида тез суръатларда оммалашмоқда.

Жумладан, харидор ва хизмат кўрсатувчилар ўз маҳсулотларини катта аудиторияга намойиш қилиш орқали осонлик билан дунёнинг турли жойларидан харидорлар топиш ва товарларини ўзи учун мақбул нархларда сотиш, харидорлар эса ўзи истаган товар ва хизматларнинг кенг миқёсдаги ассортиментидан афзалини танлаш имкониятига эга бўлмоқда.

Халқаро электралоқа иттифоқи (ХЭАИ) маълумотларига кўра, 2019 йилда дунё аҳолисининг 53,6 фоизи (4,131 миллион киши) онлайн савдо платформаларидан фойдаланган ҳолда савдоларни амалга оширган [1].

2019 йилда бутун дунё бўйлаб, онлайн савдо ҳажми 3,5 триллион АҚШ долларни ташкил этган бўлса, 2022 йилда бу кўрсаткич 6,6 триллион АҚШ долларига, 2023 йилда эса 9,3 триллион АҚШ долларга ўсган [2].

Юқоридагилардан келиб чиқиб, онлайн савдо платформалари бугунги кунда бутун дунёда, жумладан мамлакатимизда ҳам турли хизмат ва маҳсулотларни харид қилиш учун энг қулай воситалардан бири ҳисобланмоқда ҳамда унинг фойдаланувчилари сони прогрессив тарзда ўсиб бормоқда. Қатор қулайликлар билан бир қаторда ушбу савдо платформалари турли ҳуқуқбузарликларни амалга ошириш майдонига айланиб бораётганлиги дунё ҳамжамиятида мазкур йўналишлардаги илмий-тадқиқот ишларининг долзарблигини исботламоқда.

Шу ўринда, онлайн савдо платформаларнинг юзага келиш эволюциясини таҳлил қилиш орқали, унинг келгуси истиқболларини прогноз қилиш йўналишдаги ҳуқуқбузарларнинг барвақт олдини олиш механизмларини такомиллаштиришнинг нечоғлиқ долзарблигини белгилаб беради.

Шу билан бирга, онлайн савдо платформалари орқали содир этилаётган кибержиноятларни сунъий интеллект технологиялари ёрдамида фош этиш ҳамда парсинг асосида тўпланган катта ҳажмли маълумотларни таҳлил қилишнинг усуллари ва алгоритмларини ишлаб чиқиш зарурияти юзага келмоқда. Шу жиҳатдан ҳам онлайн савдо платформалари орқали содир этилган кибержиноятларни фош этишга кўмаклашувчи интеллектуал усулларини ишлаб чиқиш муҳим вазифалардан бири ҳисобланади.

Жаҳонда онлайн савдо платформалари орқали содир этилган кибержиноятларни фош этишга кўмаклашувчи ёрдамчи тизимларни яратиш

бўйича универсал ёндашувларни ишлаб чиқишга қаратилган илмий-тадқиқот ишлари олиб борилмоқда. Бу борада, жумладан графлар назарияси, сунъий нейрон тармоқ моделлари, маълумотлар таҳлилининг интеллектуал усуллари ҳамда алгоритмларидан фойдаланган ҳолда содир этилган кибержиноятларни фош этиш учун дастурий воситалар мажмуасини ишлаб чиқиш муҳим вазифалардан бири ҳисобланади.

[3]да шубҳали ҳаволалар орқали контентни филтрлайдиган техник аниқлаш тизимларини таклиф қилди. Бир неча дақиқада яратилган катта миқдордаги сохта контентлар билан курашишдаги муваффақиятларига қарамай, бу усул бугунги кунда самарасиз дея таъкидланмоқда.

Ушбу турдаги кибержиноятларни аниқлашни яхшилаш катта ҳажмдаги маълумотларини ва контекст тилини қайта ишлашни талаб қилади. Сохта онлайн савдо платформалари ёки фишинг платформаларни аниқлаш бўйича маълум техник амалий муаммолар туфайли ҳамма жойда қўлланилмайди. Онлайн савдо платформаларидаги фирибгарликни аниқлашни яхшилаш учун фойдаланувчига йўналтирилган ёндашувлар бир хил даражада муҳим бўлиб қолмоқда.

Сохта онлайн савдо платформаларини интеллектуал усуллардан фойдаланган ҳолда аниқлаш тизимлари, одатда, DMARC каби платформаларда амалга оширилади. Ушбу тизим онлайн фирибгарликларни тавсифловчи маълумотлар намуналаридан ўқитади. Масалан, эълон хабарлари ёки унда келтирилган изоҳларнинг мазмунига қараб. Назоратсиз ўқитиш, унда ишончли деб топилмаганлари ҳам ярим назорат остида ўқитиш яъни, таққосланадиган намунавий кўрсаткичлар билан қўлланилган. Масалан, Байес ёндашувлари, векторли машиналарни ўқитиш, қарор дарахтларини шакллантириш ва нейрон тармоқлар.

Фишинг онлайн савдо платформаларни аниқлаш учун машинали ўқитиш моделларининг аксарияти ўқитиш парадигмаси ва ишлатиладиган алгоритмлардан қатъи назар, тест маълумотлар тўпламида 90% дан ортиқ умумий аниқликка эришганлиги, моделни аниқлаш кўрсаткичи асосан аниқ эмаслигидан далолат беради.

Ҳозирги вақтда турли платформалардаги маълумотларни автоматик равишда парсинг қилиш учун кўплаб тайёр дастурий таъминотлар мавжуд. Бундай ахборот тизимларда турли хизматлар мавжуд бўлиб, уларда маълум бир тўлов эвазига фойдаланувчига лозим бўлган функция учун кўп функцияли ва мослашувчан таҳлил тизимига эга бўлади. All Rival ва Target Hunter парсинг қилиш тизимлари сирасига киради. Улар кўп функционал манбалардан маълумотларни тўплаш имконига эга бўлган кўп функцияли парсинг қилиш тизимидир. Дастур турли мезонларга кўра фойдаланувчилар, веб-сайтларга жойлаштирилган контентлар ҳақида маълумотлар тўплайди. Шунингдек, дастурда маълумотларни фильтрлашни мослашувчан созлаш функциясига эга.

Юқорида таҳлил қилинган онлайн савдо платформалари орқали содир этилаётган кибержиноятларни фош этишга кўмаклашувчи тизимлар маълум вазифаларнинг айрим қисмларини бажаришга мўлжалланган бўлиб, комплекс вазифаларни амалга ошириш имкони мавжуд эмас.

Шунинг учун ҳам, онлайн савдо платформалари орқали содир этилаётган кибержиноятларни фош этишга кўмаклашувчи тизимларни ишлаб чиқишда комплекс ёндашувлар асосида ишлаб чиқиш мазкур соҳадаги ишлар жадаллигини янада оширади.

Фойдаланилган адабиётлар

1. https://www.researchgate.net/publication/344771092_Msc-Computer_Science_Dissertation_Using_big_data_for_corporate_brand_analysis_on_the_internet
2. https://etheses.whiterose.ac.uk/27179/
3. https://core.ac.uk/outputs/230627840/?source=2

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО - НЕОБХОДИМОЕ УСЛОВИЕ ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ УРОВНЕ.

Якубов А.С. *доктор юридических наук, профессор.*
Азим Ш.О. *(PhD) доктор философии по юридическим наукам.*

Тенденции преступности сложны и противоречивы, что особенно наглядно выявляется при исследовании ее динамики за значительные промежутки времени. Влияние оказывают многие факторы. Одним из таких факторов выступает научно-технический прогресс и происходящие в его рамках интеллектуально-промышленные поистине революционные изменения, влекущие как появление новых сфер общественных отношений, так и усложнение уже функционирующих. При этом, что уже подтверждено практикой, научно-технический прогресс и все его составляющие обладают сильной деликтогенностью, постоянно вызывая к жизни всё новые и новые составы правонарушений, усложняя и делая более опасными уже традиционно известные. Это напрямую относится и киберпространству, в котором с геометрической прогрессией происходят постоянные трансформации, причем не только положительного свойства, но и отрицательно влияющих на функционирующие в социальной жизни общественные отношения. Всё это актуализировало проблему необходимости обеспечения охраны, профилактирования и предупреждения посягательств, осуществляемых в киберпространстве, общепризнанно обозначаемых большинством ученых и практикующих юристов как самостоятельное явление современности – киберпреступность.

Об усложнении криминогенной обстановки в киберпреступности и нарастании криминальных проявлений в этой сфере, свидетельствует значительный рост жертв от кибератак, причем как физических, так и юридических лиц, не говоря уже об имиджевых потерях государственных и других структур власти, суммы как прямых, так косвенных финансовых потерь и убытков. Так, в 2021 году количество кибератак во всем мире увеличилось на 125% по сравнению 2020 годом, и в 2022 году растущий объем кибератак

продолжал угрожать предприятиям и частным лицам. В 2023 году 50% предприятий Великобритании подверглись в той или иной форме кибератакам, против 39% в 2022 году. В первой половине 2022 года во всем мире произошло около 236,1 миллионов атак с использованием программ-вымогателей. Каждый год незаконно вскрывается около 1 миллиарда электронных писем, что затрагивает каждого пятого интернет-пользователя. Средняя сумма убытков предприятий от утечек данных ежегодно колеблется в пределах 4-4,5 миллионов долларов США и по существу ни одно из предприятий не застраховано от кибератак. Реальность угроз кибератак, возрастающая стоимость утечек данных, обусловили формирование достаточно трезвого и пристального внимания к сфере кибербезопасности. Так, почти 73% представителей малого и среднего бизнеса полагают необходимым уделять внимание этой проблематике, а 78% признали целесообразным увеличение средств и инвестиций в кибербезопасность.

При этом, несмотря на то, что 67% представителей малого и среднего бизнеса объективно признают, что у них нет внутренних условий по предотвращению утечки данных, они пытаются воздействовать на эти процессы посредством пользования услугами профессионалов, поставщиков таких услуг в сфере кибербезопасности. От осознания важности такой деятельности свидетельствует тот факт, что если в 2020 году такими услугами пользовалось 74% предпринимателей, то к 2022 году эта цифра выросла до 89%. В криминологическом исследовании 2022 года, охватившем США, Канаду, Великобританию, Австралию и Новую Зеландию, 76% респондентов отмечали, что их организация пострадала в этом году как минимум от одной кибератаки, тогда как в 2020 году такие атаки отмечали только 55% респондентов. При этом, лишь 30% организаций из опрошенных констатировали наличие киберстрахования. В опубликованных источниках приводятся сведения об атаках на организации по континентам за 2021 год в процентном отношении по количеству: Азия - 26%; Европа - 24%; Северная Америка - 23%; Ближний Восток и Африка -14%; Латинская Америка-13%.

Следует констатировать растущие издержки киберпреступности, поскольку методы атак становятся все более изощренными и профессиональными. Это побуждает организации по всему миру инвестировать дополнительные средства и ресурсы в современные меры безопасности, включая обновленные программы обучения персонала, введение штата специальных сотрудников по киберпреступности и др. По оценкам специалистов, средняя стоимость одного кибернарушения в 2020 году оценивалась в 4,35 миллионов долларов США. Констатируется, что киберпреступность обойдется мировой экономике примерно в 7 триллионов долларов США. В 2022 году прогнозируется, что к 2025 году эта цифра возрастет до 10,5 триллионов долларов США.

В мировом сообществе, с учетом накопленного опыта, констатируется несколько преступных проявлений киберпреступности. Самой распространённой киберугрозой, с которой сталкиваются организации и частные

лица, является фишинг[3]. В 2021 году 323 972 интернет-пользователей сообщили о том, что стали жертвами фишинговых атак, что по разным оценкам составляет почти половину пользователей, пострадавших от утечки данных. В этот период констатировано около одного миллиарда электронных писем, которые затронули каждого пятого пользователя интернета.

Фишинг является наиболее распространенной формой кибератак, поскольку подтверждено, что ежедневно отправляется около 3,4 миллиарда спам-писем. Фишинг зачастую представляет собой атаку «входа», когда киберпреступники собирают конфиденциальную информацию (например, данные для ввода или номера кредитных карт), которую затем возможно использовать для запуска дальнейших атак. Установлено, что фишинг является наиболее распространенной точкой входа для атак с использованием программ-вымогателей, когда рассылается спам будущим жертвам до тех пор, пока адресат не перейдет по соответствующей ссылке, которая может содержать программу-вымогатель или перенаправить ее на поддельный веб-сайт, где потерпевший вольно или невольно вводит свои данные для входа. Эти данные впоследствии используются для получения внутреннего доступа к сети, либо эскалации своей атаки и внедрения программы-вымогателя.

Одной из разновидностей кибератак являются программы-вымогатели, которые представляют серьезную угрозу как для отдельных лиц, так и для организаций, посредством которых, потерпевших вынуждают платить. В первой половине 2022 года по всему миру было зарегистрировано около 236,1 миллиона атак с использованием программ-вымогателей.

Распространенным является шантажирование потенциальных жертв посредством угроз публикации конфиденциальных фотографий, видео или иной информации, связанной с сексуальными действиями, при условии невыполнения определенных противоправных действий (Sextortion). Так, по данным Департамента IC3 США, в 2021 году поступило более 18 тысяч жалоб, связанных с сексуальным вымогательством, а убытки пострадавших составили более 13,6 миллионов долларов США.

К числу разновидностей киберпреступности относятся финансовое мошенничество, мошенничество в розничной торговле и продаже потребительских товаров, любовные аферы, взлом деловой электронной почты, киберпреследования, кибер клевета, кража личных данных, взлом социальных сетей, романтические аферы, и др.

Весьма распространенным стали атаки на «цепочки поставок». Цепочки поставок становятся все более взаимосвязанными и сложными по мере совершенствования технологий. Такая связь представляет определенные риски, если предприятия и организации незащищены должным образом, что повышает уязвимость безопасности партнёров. Киберпреступники нацелены на эти

[3] Фишинг – вид интернет мошенничества, целью которого является получение доступа к конфиденциальным данным пользователя - логинам и паролям. Это достигается посредством проведения массовой рассылки электронных писем от имени популярных брендов, а также личных сообщений внутри различных серверов (например, от имени банков или внутри социальных сетей).

уязвимости, и до 40% киберугроз происходит косвенно, именно через цепочку поставок.

Здесь провоцирующими выступают как человеческий фактор – недостаточный мониторинг партнеров и поставщиков в режиме реального времени на предмет рисков кибербезопасности, так и недостаточное внимание компаний в инвестиции в систем безопасности, включая современное программное обеспечение и специальных подразделений, обеспечивающих безопасное функционирование предприятия.

В современной литературе киберпреступность условно подразделяют на две категории:

а) киберзависимая преступность, то есть преступления, которые можно совершить только с использованием технологий, когда устройства являются как инструментом совершения преступлений, так и его целью (вредоносные программы, взломы с целью удаления или повреждения данных и др.);

б) традиционная преступность, расширившая своё влияние за счет использования современных технологии (кибермошенничество, кражи и др.).

Достаточно распространённым преступлением, совершаемым с использованием интернета, является мошенничество. Риски, сопряжённые с возможностью быть вовлечённым в различного рода мошеннические схемы, возникают при инвестировании денежных средств на иностранных фондовых рынках с использованием сети интернет. Распространенной разновидностью мошенничества являются звонки по телефону, когда предпринимаются попытки у владельцев банковских карт получения конфиденциальной информации, осуществить перевод либо установить программы удаленного доступа.

Другой вид мошенничества осуществляется на интернет-аукционах, когда сами продавцы завышают ставки с тем, чтобы поднять цену выставленного на аукцион товара. Продажа доменных имён, как разновидность кибермошенничества заключается в массовой рассылке электронных сообщений, в которых, например, сообщается о попытках неизвестных лиц зарегистрировать доменные имена, похожие на принадлежащие адресатам сайты, с предложениями о регистрации ненужное адресатам доменного имени, с целью их опережения.

Для полноты криминологической характеристики киберпреступности важно акцентировать внимание на профессиональном характере преступных посягательств, на безопасность в сфере информационных технологий. Основываясь на этом предварительном замечании следует констатировать, что с криминологической, и с уголовно-правовой позиции, мы имеем дело с таким явлением современности, как организованная преступность. В литературе отмечается, что организованная преступность «… являясь одной из форм преступности, характеризуется высокой комплексной общественной опасностью и проявляется в системе деятельности всех преступных организаций данного региона за определенный период»[4], либо «…обладающая высокой степенью общественной опасности форма социальной патологии, выражающаяся в

[4] Уголовное право. Общая часть. – Т., Академия МВД Республики Узбекистан, 2005. – С.309.

постоянном и относительно массовом воспроизводстве и функционировании устойчивых преступных сообществ (преступных организаций)»[5].

Представляется что, наиболее существенными признаками организованной преступности являются: а) наличие преступных организаций (объединений) различной степени сплоченности, имеющих функционально- иерархическую структуру со строгой субординацией и координацией функций между лицами или группами; б) наличие профессионалов, для которых преступная деятельность является основной формой существования и образа жизни; в) устойчивый, планируемый, законспирированный характер преступной деятельности; г) наличие систем обеспечения преступной деятельности, собственной безопасности и нейтрализации социального контроля; д) значительные денежные фонды, инвестируемые в преступную деятельность, легальный бизнес, доходы от которого направляются на коррумпирование государственных чиновников, материальную поддержку осужденных и т.д.; е) прогрессирующая тенденция к расширению сфер преступной деятельности и влияния преступных организаций; ж) антиобщественная идеология, своего рода «кодекс» поведения.

По мнению Э.Ф.Побегайло, к наиболее типичным признакам организованной преступности относятся: участие значительного числа лиц; устойчивость криминальных связей между членами групп; наличии специфических норм и правил поведения в среди её функционеров; специализация преступной деятельности; её предумышленный и заранее спланированный характер; иерархическая структура преступных групп и распределение ролей их участников; систематический преступный бизнес (промысел); межрегиональные связи; повышенная конспиративность; коррумпирование представителей власти и некоторые другие.

С позиции нашего анализа важно подчеркнуть, что киберпреступность в обязательном порядке характеризуется и международными связями.

Представляется правильным выделение двух разновидностей организованной преступности: общеуголовной и хозяйственно-экономической, последняя из которых, образуя разновидность профессиональной преступности, непосредственно свойственна и должна характеризировать киберпреступность.

Таким образом, преступления в сфере информационных технологий предполагают, как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, фишинг, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, направленных на возбуждение межнациональной и межрелигиозной вражды и т.п.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

Как показывает практика, преступления в сфере информационных технологий имеют международный характер, поскольку, как правило,

[5] Побегайло Э.Ф. Тенденции современной преступности и совершенствование уголовно-правовой борьбы с нею. М., 1990. – С.17.

совершаются на территории нескольких государств, что актуализирует значение международного сотрудничества.

В качестве правовой основы международного сотрудничества в сфере борьбы с киберпреступностью может служить Конвенция Совета Европы о преступности в сфере компьютерной информации (ETS №185), подписанная 23 ноября 2001 года в Будапеште[6]. Она открыта для подписания как государствами-членами Совета Европы, так и странами, которые не являются членами, но которые приняли участие в составлении и во вступлении других стран не членов.

Конвенция Совета Европы о компьютерных преступлениях (ETS №185) подразделяет преступления в киберпространстве на четыре группы.

Первую группу преступлений, направленных против конфиденциальности, целостности и доступности компьютерных данных и систем, входят: незаконный доступ (ст.2), незаконный перехват (ст.3), воздействие на компьютерные данные (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокировка компьютерных данных) (ст.4) или системы (ст.5).Также в эту группу преступлений входит противозаконное использование специальных технических устройств (ст.6) - компьютерных программ, разработанных или адаптированных для совершения преступлений, предусмотренных в ст.ст. 2-5, а также компьютерных паролей, кодов доступа, их аналогов, посредством которых может быть получен доступ к компьютерным системам в целом или любой ее части. Нормы ст. 6 подлежат применению только в случаях, если использование (распространение) специальных технических устройств направлено на совершение противоправных деяний.

Во вторую группу входят преступления, связанные с использованием компьютерных средств. К ним относятся подлог и мошенничество с использованием компьютерных технологий (ст.ст.7,8). Подлог с использованием компьютерных технологий включает в себя злонамеренные и противоправные ввод, изменение, удаление или блокирование компьютерных данных, влекущих за собой нарушение аутентичности данных, с намерением, чтобы они распространялись или использовались в юридических целях в качестве аутентичных.

Третью группу составляет производство (с целью распространения через компьютерную систему), предложение и (или) предоставление в пользование, распространение и приобретение порнографии и детской порнографии, а также владение детской порнографии, находящейся в памяти компьютера (ст.9).

Четвёртую группу составляют преступления, связанные с нарушением авторского права и смежных прав.

В начале 2002 года был принят Протокол № 1 к Конвенции о киберпреступности, в соответствии с которым к категории преступлений было отнесено распространение информации расистского и другого характера, подстрекающего к насильственным действиям, ненависти или дискриминации

[6] The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols https://www.coe.int/en/web/cybercrime/the-budapest-convention

отдельного лица или группы лиц, основывающегося на расовой, национальной, религиозной или этнической принадлежности.

В соответствии с положениями Конвенции, каждое государство- участник обязано создать необходимые правовые условия для предоставления следующих прав и обязанностей компетентным органам по борьбе с киберпреступностью: выемка компьютерной системы, её части или носителей; изготовление или конфискация копии компьютерных данных; обеспечение целостности и сохранности хранимых компьютерных данных, относящихся к делу; уничтожение или блокирование компьютерных данных, находящихся в компьютерной системе.

Конвенция также определяет создание необходимых условий для обязанности интернет-провайдеров проведения необходимого сбора и фиксации или перехвата необходимой информации с помощью имеющихся технических средств, а также способствовать в этом правоохранительным органам. При этом рекомендуется обязать провайдеров сохранять полную конфиденциальность о фактах подобного сотрудничества.

В Республике Узбекистан сформирована правовая основа борьбы с киберпреступностью. В соответствии с Законом Республики Узбекистан от 25 декабря 2007 года (ЗРУ-137)[7] Уголовный кодекса был дополнен самостоятельной Главой XX[1], предусматривающей ответственность за преступления в сфере информационных технологий, а в некоторые другие статьи Особенной части были включены в качестве квалифицирующих и особо квалифицирующих признаков преступления, совершаемые с использованием средств компьютерной техники, сетей телекоммуникаций, а также всемирной информационной сети Интернет.

По УК РУз преступлениями в сфере компьютерной информации являются: нарушение правил информатизации (ст.278[1]), незаконный (несанкционированный) доступ к компьютерной информации (ст.278[2]), изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций (ст.278[3]), модификация компьютерной информации (ст.278[4]), компьютерный саботаж (ст.278[5]), создание, использование или распространение вредоносных программ (ст.278[6]), незаконный (несанкционированный) доступ к сети телекоммуникаций (ст.278[7]).

Данная группа посягательств является институтом Особенной части, отнесённой по родовой принадлежности к преступлениям против общественного порядка и общественной безопасности. Видовым объектом выступает общественная безопасность при непосредственном посягательстве на общественные отношения, связанные с безопасностью информации и систем обработки информации с помощью ЭВМ. Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение

[7] См.: Собрание законодательства Республики Узбекистан, 2007 г., № 52, ст.532.

деятельности автоматизированных систем управления и контроля различных объектов, серьёзное нарушение работы сетей телекоммуникаций, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и физическим вредом людям.

В соответствии с Законом Республики Узбекистан от 13 июня 2017 года (ЗРУ-436)[8] такое преступление против жизни как доведение до самоубийства (ст.103 УК) была дополнена квалифицирующим признаком, повышающим ответственность, если доведение до самоубийства или покушение на него путём угроз, жестокого обращения или систематического унижения чести и достоинства личности лица осуществлялось с использованием сетей телекоммуникаций, а также всемирной информационной сети Интернет. Этим же Законом склонение к самоубийству (ст.103_1 УК) было криминализировано, а использование при этом сетей телекоммуникаций и всемирной информационной сети Интернет оценено законодателем как квалифицированный состав.

Корректировке подверглись и некоторые преступления в сфере экономики, представляющие хищения чужого имущества. В нормах, предусматривающих ответственность за хищение путем присвоения или растраты (ст. 167), мошенничество (ст. 168), кражу (ст. 169) предусматривается повышенная ответственность, если они совершены с использованием средств компьютерной техники или с несанкционированным проникновением в компьютерную систему.

Необходимость действенной охраны отношений в сфере хозяйственной деятельности обусловило установление уголовной ответственности за незаконную деятельность по привлечению денежных средств и (или) иного имущества (ст.188^{1})[9], где в качестве конструктивного и квалифицирующего предусмотрен признак «с использованием средств массовой информации либо коммуникаций, а также всемирной информационной сети Интернет».

Следует отметить как позитивное в законодательном процессе своевременное реагирование и установление уголовной ответственности за использование или хранение с целью распространения материалов, содержащих идеи религиозного экстремизма, сепаратизма и фундаментализма, призывы к погромам или насильственному выселению граждан либо направленных на создание паники среди населения, а также изготовление, хранение с целью распространения либо демонстрации атрибутики или символики религиозно-экстремистских, террористических организаций, а равно распространение таких сведений либо использование религии в целях нарушения гражданского согласия, распространение клеветнических, дестабилизирующих обстановку измышлений и совершение иных действий, направленных против установленных правил поведения в обществе и общественной безопасности (ч.

[8] См.: Собрание законодательства Республики Узбекистан, 2017 г., № 24. Ст.487.

[9] См.: Собрание законодательства Республики Узбекистан от 23 сентября 2016 года № ЗРУ-411. Собрание законодательства Республики Узбекистан, 2015 г., № 39. Ст.457.

1.2. ст. 244[1] УК), отягощённые тем, что эти действия осуществлялись с использованием средств массовой информации либо сетей телекоммуникаций, а также всемирной информационной сети Интернет (п.«г» ч.3. ст. 244[1] УК).

В современном, постоянно меняющемся мире, совершенствование технологий, необходим постоянный мониторинг как со стороны технических специалистов, так и со стороны правоведов. Совершенствующиеся методы криминальных проявлений в сфере кибербезопасности требуют своевременного реагирования и в первую очередь на законодательном уровне. Так, например, получающие всё большую распространённость технологии Deepfake, посредством которых с помощью искусственного интеллекта (ИИ) создают ложные видеообращения, генерации похожести голосов с целью осуществления мошеннических действий уже сегодня требует законодательного реагирования.

Общепризнанно, что преступления в сфере информационных технологий очень часто является международными. Учитывая это, следует обратить внимание на такой институт Общей части УК как действие уголовного закона в пространстве. В международной законотворческой практике наряду с территориальным, гражданства и универсальным принципами действия уголовного закона в пространстве, которые присуще и законодательству Узбекистана, предусматривается также и реальный принцип. Как отмечается в литературе, сущность реального принципа действия уголовного закона в пространстве состоит в том, что государство признаёт возможным привлечение к уголовной ответственности иностранных граждан и лиц без гражданств или без гражданства, постоянно не проживающих на его территории, за преступления, направленные против интересов этого государства даже если эти преступления не совершены на его территории и не предусмотрены международными договорами.[10] Поскольку при киберпреступности нередки случаи совершения посягательств на интересы республики Узбекистан и его граждан вне пределов и территории нашего государства необходимо распространить действия УК РУз и на такие криминальные проявления. На основании изложенного предлагается новая редакция ч.3 статьи 12 УК: «иностранные граждане и лица без гражданства, не проживающие постоянно на территории Республики Узбекистан, подлежат уголовной ответственности по настоящему Кодексу в случаях, если преступление направлено против интересов Республики Узбекистан, и в случаях, предусмотренном международном договором Республики Узбекистан, если они не были осуждены в иностранном государстве и привлекаются к уголовной ответственности на территории Республики Узбекистан».

Использованная литература:

1. Закон Республики Узбекистан, от 15.04.2022 г. № ЗРУ-764 «О кибербезопасности» URL: https://lex.uz/ru/docs/5960609
2. Уголовное право. Общая часть. – Т., Академия МВД Республики Узбекистан, 2005.

[10] См.: Уголовное право. Общая часть. – Т., 2005. – С.112.

3. Побегайло Э.Ф. Тенденции современной преступности и совершенствование уголовно-правовой борьбы с нею. М., 1990.
4. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols https://www.coe.int/en/web/cybercrime/the-budapest-convention
5. Собрание законодательства Республики Узбекистан, 2007 г., № 52.
6. См.: Собрание законодательства Республики Узбекистан, 2017 г., № 24.
7. См.: Собрание законодательства Республики Узбекистан от 23 сентября 2016 года № ЗРУ-411.
8. Собрание законодательства Республики Узбекистан, 2015 г., № 39.

OBYEKTLARNI QO‘RIQLASHDA SITUATSION-TAHLILIY MARKAZLARNING AHAMIYATI

Marupov Erkinjon Elmirovich

O‘zbekiston Revpublikasi Malaka oshirish instituti Axborot texnologiyalari sikl boshlig‘i

Annotatsiya: Situatsion-tahliliy markazlari (keyingi o‘rinda - Markaz) ma’lumotlarni keng qamrovli tahlil etish, xavf-xatarlarni oldindan ko‘ra bilish va samarali qarorlar qabul qilish vositalarini ta’minlash orqali obyektlarni qo‘riqlashda muhim ahamiyat kasb etadi. Maqolada zamonaviy qo‘riqlanadigan obyektlarning xavfsizligini ta’minlashda Markazlarining o‘rni yoritilgan. Markazlarning tuzilmasi, ish tartibi, vazifalari va maqsadlari, shuningdek, ularning turli xavfsizlik quyi tizimlari, jumladan videokuzatuv, kirish nazorati, signalizatsiya, yong‘inga qarshi tizimlar batafsil tavsiflangan. Bu tizimlar obyekt holatini tezkor kuzatish va potentsial tahdidlarni aniqlash imkonini beruvchi ma’lumotlarni markazlashtirish uchun xizmat qiladi. Bundan tashqari, Markazlaridan foydalanishning afzalliklari va ularning rivojlanish yo‘nalishlari bayon etilgan.

Kalit so‘zlar: Situatsion-tahliliy markazlari, asosiy funksiyalar, foydalanish afzalliklari, rivojlanish tendensiyalari.

Zamonaviy qo‘riqlanadigan obyektlarning xavfsizligini ta’minlashda Situatsion-tahliliy markazlari (keyingi o‘rinda - Markaz) hal qiluvchi ahamiyatga ega. Ular turli xil xavfsizlik quyi tizimlaridan, jumladan videokuzatuv, kirish nazorati, signalizatsiya, yong‘inga qarshi tizimlar va boshqalardan olingan ma’lumotlarni birlashtiruvchi yaxlit axborot-tahliliy majmualardir. Bunday ma’lumotlarni markazlashtirish obyekt holatini tezkor kuzatish va mumkin bo‘lgan xavf-xatarlarni aniqlash imkonini beradi.

Obyektlarni qo‘riqlashda Markazlarning asosiy funksiyalari:

- **Ma’lumotlarni to‘plash va qayta ishlash:** Markazlar turli manbalardan, jumladan videokuzatuv tizimlari, kirish nazorati tizimlari, sensorlar, shuningdek tashqi ma’lumotlar bazalari va ochiq axborot manbalaridan ma’lumotlarni to‘playdi va ularni qayta ishlaydi.

• **Tahdidlarni tahlil qilish va baholash:** Markazlar potensial xavflarni ko‘rsatishi mumkin bo‘lgan qonuniyatlar, tendensiyalar va g‘ayrioddiy holatlarni aniqlash uchun Big Data va Data Mining singari zamonaviy ma’lumotlarni tahlil qilish usullaridan foydalanadilar. Bu usullar yordamida ular katta hajmdagi ma’lumotlarni qayta ishlab, muhim ma’lumotlarni olishadi.

• **Ma’lumotlarni vizualllashtirish:** Markazlar interaktiv xaritalar, grafiklar, diagrammalar va boshqa ko‘rgazmali vositalardan foydalanib, ma’lumotlarni tushunish uchun qulay shaklda taqdim etadi.

• **Qaror qabul qilishni qo‘llab-quvvatlash:** Markazlar qaror qabul qiluvchi shaxslarga tahdidlarga tezkor munosabat bildirish va asosli qarorlar qabul qilish uchun zarur bo‘lgan barcha ma’lumotlarni yetkazib beradi.

Markazlarning obyektlar xavfsizligini oshirishga qo‘shgan hissasi:

• **Tezkor munosabat bildirish:** Markazlar tahdidlarni o‘z vaqtida aniqlash va baholashni ta’minlaydi, bu esa hodisalarga javob berish vaqtini qisqartiradi.

• **Resurslardan samarali foydalanish:** Markazlar ma’lumotlarni tahlil qilish va tahdidlarni bashorat qilish asosida qo‘riqlash kuchlari va vositalarini optimal taqsimlashga ko‘maklashadi.

• **Hodisalarning oldini olish:** Markazlar tomonidan ishlab chiqilgan bashorat modellari xavf omillarini aniqlash va bartaraf etish orqali hodisalarning yuzaga kelishini oldini olish imkoniyatini beradi.

• **Hamkorlik samaradorligini oshirish:** Markazlar turli tizim va xizmatlardan olingan ma’lumotlarni birlashtiradi, bu esa harakatlarni muvofiqlashtirishni yaxshilash va hamkorlik samaradorligini oshirishga yordam beradi.

Markazlardan foydalanishning afzalliklari:

• **Xavfsizlik darajasini oshirish:** Markazlar turli tizimlarni birlashtirish va tahdidlarga tezkor javob berish orqali xavfsizlikka keng qamrovli yondashuvni ta’minlaydi.

• **Xavflarni kamaytirish:** Tahdidlarni o‘z vaqtida aniqlash va hodisalarni oldindan ko‘ra bilish profilaktika choralarini ko‘rish hamda xavflarni kamaytirishga imkon yaratadi.

• **Xarajatlarni optimallashtirish:** Markazlashtirilgan boshqaruv va jarayonlarni avtomatlashtirish resurslardan yanada samarali foydalanishga ko‘maklashadi.

• **Boshqaruv sifatini oshirish:** Markazlar asosli qarorlar qabul qilishga yordam beradigan ma’lumotlar, tahliliy vositalar va modellashtirish imkoniyatlaridan tezkor foydalanishni ta’minlaydi.

Markazlarning rivojlanish yo‘nalishlari:

• **Tarqoq Markazlar tizimi:** Turli darajadagi markazlarni ma’lumot almashish va harakatlarni muvofiqlashtirish uchun yagona tarmoqqa birlashtirish.

• **Tashqi axborot tizimlari bilan uyg‘unlashtirish:** Vaziyatni yanada to‘liqroq tahlil qilish maqsadida ijtimoiy tarmoqlar, yangilik saytlari, ob-havo xizmatlari va boshqa manbalardan olingan ma’lumotlardan foydalanish.

• **Katta hajmli ma’lumotlar va ma’lumotlarni qazib olish:** Yashirin qonuniyatlarni aniqlash, xavf-xatarlarni oldindan aytib berish va qarorlar sifatini oshirish uchun katta hajmli ma’lumotlarni tahlil qilish texnologiyalarini qo‘llash.

• **Tahliliy vositalarni takomillashtirish:** Ma’lumotlarni tahlil qilish va bashorat qilish samaradorligini oshirish uchun yangi tahliliy vositalar va usullarni joriy etish.

Markazlarni tashkil etish va qo‘llash bo‘yicha zamonaviy yondashuvlar:

• **Sun’iy intellektdan (SI) foydalanish:** Markazlar ma’lumotlarni tahlil qilish, tahdidlarni aniqlash va qaror qabul qilish jarayonlarini avtomatlashtirish uchun SI texnologiyalaridan tobora ko‘proq foydalanmoqda.

• **Biznes tahlili (Business Intelligence - BI) tizimlari bilan integratsiyalash:** BI tizimlari tahlil va bashoratlash samaradorligini oshirish maqsadida Markazlar bilan birlashtirish mumkin bo‘lgan ma’lumotlarni tahlil qilish uchun keng qamrovli vositalarni taqdim etadi.

• **Maxsus dasturiy majmualarni ishlab chiqish:** Obyektlarni qo‘riqlashning o‘ziga xos vazifalarini hal etish uchun maxsus dasturiy majmualar ishlab chiqilmoqda.

Xulosa. Qo‘riqlanadigan obyektlarning xavfsizligini ta’minlashda Situatsion-tahliliy markazlari muhim ahamiyatga ega. Sun’iy intellekt va BI kabi zamonaviy texnologiyalar obyektlarning xavfsizlik darajasini sezilarli darajada oshirishga qodir bo‘lgan yanada samaraliroq markazlarni yaratish imkonini bermoqda. Bu markazlar xavfsizlik masalalarini kompleks hal etish vositalarini taqdim etib, qarorlar qabul qilish jarayonining samaradorligi, tezkorligi va sifatini oshiradi. Texnologiyalarning rivojlanishi va xavfsizlik vazifalarining murakkablashuvi natijasida Markazlar doimiy ravishda takomillashib, ularning funksional imkoniyatlari kengayib, yagona axborot tizimlariga integratsiyalashuvi kuchayib bormoqda.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1) Кухаренко Н.С. Рол ситуационных центров в деятелности органов государственной власти при чрезвычайных ситуациях // Сетевое издание «Академическая мысл» № 1 (14) 2021. – С. 35–38.

2) Пянков О.В., Попов А.В. Информационная модел принятия решений в ситуационных центрах органов внутренних дел // Вестник Воронежского института МВД России № 2 / 2020. – С. 59–68.

3) Захаренков А.И., Соколов А.В. Метод извлечения информации из массивов неструктурированных текстов // Инновации в информационно-аналитических системах: сб. научн. трудов. Вып. 5 – Курск: Науком, 2013. - С. 44–54, ил. ISBN 978-5-4297-0009-0

4) Кониченко А.В., Миргалеев А.Т., Уваров А.Н. Разработка эксперименталного образца программного комплекса информационно-аналитической системы // Инновации в информационно-аналитических системах: сб. научн. трудов. Вып. 6 – Курск: Науком, 2013. - С. 5–25, ил. ISBN 978-5-4297-0010-6

5) Пянков О.В. Ключевые показатели исползования информационно-аналитических систем органов внутренних дел // Вестник Воронежского института МВД России №4 / 2015. - С. 155–162

6) Пянков О.В. Информационно-аналитическая система: назначение, рол, свойства // Информационная безопасност регионов. 2014. № 1(14). - С. 21–26

7) Удалов В. П. Эффективност метода экспертного оценивания модели надежности технической системы безопасности // Вестник Воронежского института МВД России № 2 / 2019. - С. 113–122
8) Менших В.В., Самороковский А.Ф., Корчагин А.В. Модел действий органов внутренних дел в чрезвычайной ситуации техногенного характера.
9) Филяк П.Ю., Байларли Э.О., Растворов В.В., Старченко В.И. Инструменталные средства для исползования Big Data и Data Mining в целях обеспечения информационной безопасности – подходы, опыт применения // Вестник МФЮА № 2 / 2017. – С. 210-220
10) Денисов Д.Ю. Ситуационные центры как инструмент современной системы менеджмента // Креативная экономика.–2021. – Том 15. – № 12. –С. 4825–4836. doi: 10.18334/ce.15.12.113849
11) Абрамов В.И., Евдокимов Д.С. СИТУАЦИОННЫЙ ЦЕНТР КАК МЕХАНИЗМ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ: РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ // РППЭ. 2019. №10 (108). URL: https://cyberleninka.ru/article/n/situatsionnyy-tsentr-kak-mehanizm-gosudarstvennogo-upravleniya-rossiyskiy-i-zarubezhnyy-opyt (дата обращения: 02.12.2024).
12) https://htm-s.ru/solutions/situatsionnye-tsentry/situatsionnye-tsentry/
13) https://www.tadviser.ru/index.php
14) https://www.connect-wit.ru/situatsionnye-tsentry-sistemnyj-podhod.html

KIBERXAVFSIZLIKNI OLDINI OLISHDA SHAXS HUQUQIY IJTIMOIYLASHUVINING O‘RNI

Atamirzaev Ibroxim Xakimovich

Namangan davlat universiteti Yuridik fakulteti dekan o‘rinbosari yu.f.d. (PhD)

Bugun jaxonda axborot texnologiyalarining rivojlanishi, XXI asr – axborot texnologiyalar asri bo‘lganligi, insonlarga qanchalik qulay bo‘lgan bo‘lsa, shunchalik ularning hayoti va shaxsiy ma’lumotlariga bo‘lgan xafvsizlikning kamayishiga olib keldi. Insonlar o‘rtasida elektron pullar ishlatilib ularning qancha qulayligi ortgan bo‘lsa, ularga nisbatan hujum ham shu darajada ortdi. Aynan ushbu sohalardagi xafvsizlik “Kiberxafvsizlik” bilan ta’minlanadi.

Shuningdek kibermakonda sodir bo‘layotgan jinoyatlar soni hozirgi kunga sezilarli darajada oshib bormoqda. Kibermakondagi jinoyatlarning boshqa jinoyatlardan farqi bu jinoyatni shaxs masofadan sodir qiladi, inson bu jinoyatni o‘z ko‘zi bilan ko‘rmaydi, bu jinoyatda inson hayotiga emas balki ma’lumotlariga hujum bo‘ladi. Shuning uchun bu kabi jinoyatlarga qarshi kurashish uchun mamlakatda samarali ish olib boruvchi organlar tizimini yaratish bugungi kunning kechiktirib bo‘lmas vazifasi hisoblanadi.

Yangilanayotgan O‘zbekistonda ham bugungi kunga qadar “Kiberxafvsizlik” masalasi bo‘yicha qonun hujjatlari yetarli darajada emas edi. Chunku bu tushuncha va bu kabi jinoyatlar yaqin o‘tgan yillarda juda avj olib ketdi. Shu sababli O‘zbekiston Respublikasida kiberxavfsizlik sohasidagi munosabatlarni tartibga solish,

kiberjinoyatlarni oldini olish, kiberhujumdan himoyalanish maqsadida O‘zbekiston Respublikasi Oliy Majlisi tomonidan 2022 yil 15 aprelda “Kiberxafvsizlik to‘g‘risida” gi O‘zbekiston Respublikasi qonuni qabul qilindi.[1]

Mazkur qonunda axborotlashtirish ob’ekti, kiberjinoyatchilik, kibermakon, kibertahdid, kiberxavfsizlik, kiberxavfsizlik hodisasi, kiberxavfsizlik ob’ekti, kiberxavfsizlik sub’ekti, kiberhimoya kiberhujum, muhim axborot infratuzilmasi, muhim axborot infratuzilmasi ob’ektlari, muhim axborot infratuzilmasi sub’ektlari tushunchalari mazmun moxiyati ochib berildi.

Shuningdek qonun qonuniylik, kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi, kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv, kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi, O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi kabi prinsiplar bilan mustaxkamlandi.

O‘zbekiston Respublikasida kiberxavfsizlik sohasidagi yagona davlat siyosatini O‘zbekiston Respublikasi Prezidenti belgilaydi. O‘zbekiston Respublikasi Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organidir.

O‘zbekiston Respublikasi Davlat xavfsizlik xizmatiga kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlarni va davlat dasturlarini ishlab chiqishi, kiberxavfsizlik to‘g‘risidagi qonunchilik hujjatlarining ijro etilishi ustidan nazoratni amalga oshirishi, kiberxavfsizlik hodisalari yuzasidan tezkor-qidiruv tadbirlarini, tergovga qadar tekshiruvlarni va tergov harakatlarini amalga oshirish, kiberxavfsizlik hodisalarining oldini olish, ularni aniqlash va bartaraf etish hamda ularga nisbatan tegishli chora-tadbirlarni, shu jumladan ularning oqibatlarini tugatish bo‘yicha tashkiliy-texnik chora-tadbirlarni ko‘rishi, favqulodda vaziyatlarda axborot tizimlari va resurslarini kiberhimoya qilish hamda kiberxavfsizlik sohasidagi boshqa masalalar bo‘yicha chora-tadbirlarni o‘z ichiga olgan rejalarni ishlab chiqishi, kiberxavfsizlikni ta’minlashga doir ishlarni, shuningdek muhim axborot infratuzilmasi obektlarida kiberhujumlarning oldini olishga, ularni aniqlashga va ularning oqibatlarini tugatishga doir ishlarni tashkil etishi, muhim axborot infratuzilmasi obektlarining kiberxavfsizligini ta’minlashga doir talablarni belgilashi kabi bir qancha yangi vazifalar yuklatildi.

Kiberxafvsizlikni ta’minlash maqsadida kiberxafvsizlik subektlarining o‘z kiberxavfsizligini ta’minlash maqsadida vakolatli davlat organidan kibertahdidlar, dasturiy ta’minotdagi, uskunalar va texnologiyalardagi zaifliklar to‘g‘risidagi ma’lumotlarni olishi, kiberhujumlardan himoya qilish vositalari va usullari, shuningdek ularni aniqlash hamda bartaraf etish usullari to‘g‘risida vakolatli davlat organidan ma’lumotlar va maslahatlar olishi o‘z kiberxavfsizligini ta’minlash bo‘yicha chora-tadbirlarni ishlab chiqish va amalga oshirishi kabi huquqlari belgilandi.

Shuningdek qonunda **kiberxavfsizlik sub’ekti** sifatida milliy axborot resurslariga ega bo‘lish, ulardan foydalanish va ularni tasarruf etish hamda ulardan foydalanish bo‘yicha elektron axborot xizmatlari ko‘rsatish, axborotni himoya qilish hamda kiberxavfsizlik bilan bog‘liq muayyan huquqlar va majburiyatlarga ega bo‘lgan yuridik shaxs va (yoki) yakka tartibdagi tadbirkor, shu jumladan muhim axborot infratuzilmasi sub’ektlari kiritilgan.

Shuningdek **kiberxavfsizlik sub'ekti** - bu kiberxavfsizlik sohasidagi qarorlar qabul qilishi va kiberhavfsizlik sohasidagi xavfsizlikni ta'minlash uchun javobgar bo'lgan shaxs yoki tashkilot. Bu sub'ektlar kiber hujumlar, ma'lumotlarning noqonuniy yoki zararli ishlatilishi, tizimlarga kirish yoki ishlashga xalaqit berish kabi xavflardan muhofaza qilish maqsadida turli chora-tadbirlarni amalga oshiradilar.

Kiberxavfsizlik sub'ektlariga yanada batafsil to'htaladigan bo'lsak, birinchi navbatda **shaxslar masalasi e'tiborni tortadi.**

Bunda shaxs - ma'lum bir tashkilot yoki fuqarolar, ular kiberxavfsizlik sohasidagi belgilangan qoidalarga rioya qilishlari va xavfsizlikni ta'minlashga mas'ul bo'lishlari mumkin.Belgilangan qoidalarga rioya qilishda albatta shaxsdan huquqiy bilim va ko'nikma talab etiladi.

Jamiuat taraqqiuotida shaxsning o'rnini aniqlashning hozirgi talablariga uuqoridagi uondashuvlarning ikkinshisi ko'proq mos keladi, shunki zamonaviu fanlarda ijtimoiulashuv insonning madaniuatni o'zlashtirish jarauonidagi rivojlanish va o'zgarishi bilan belgilanadi.[2]

Shaxsning ijtimoiulashuvi shundau jarauonki, u insonning butun hauoti davomida u uoki bu darajada shakllanib boradi. U shaxs rivojining bolalik, o'smirlik, o'rta uosh va keksalik kabi bosqishlarida turli darajada namouon bo'ladi.[3]

Buning barobarida shaxsning ijtimoiulashuvi uning ijtimoiu adolatga oshiftaligi va intilishida namouon bo'lishini ta'kidlash joiz. Davlatimiz rahbari Sh.Mirziuouev mazkur hodisani quuidagisha keng qamrovli ifodalaudi: Ijtimoiu adolat – bu siuosiu qarashlar, jinsi, millati, tili va diniu ye'tiqodidan qat'i nazar, qonun oldida barsha fuqarolarning tengligini ta'minlashdir. Bu – ta'lim, tibbiuot va boshqa sohalardagi imkoniuatlar tengligidir. Bu – kafolatlangan mehnat faoliuati yerkinligi, mansab lavozimlari bo'uisha ko'tarilib borishdagi imkoniuatlar tengligidir. Yeng muhimi, bu – keksa avlod vakillari va ijtimoiu himouaga muhtoj fuqarolar to'g'risidagi g'amxo'rlikdir.[4]

Kiberxavfsizlik va **shaxs huquqiy ijtimoiylashuvi** o'rtasidagi bog'lanish, asosan axborot xavfsizligini ta'minlash va shaxsning huquqlarini himoya qilishga qaratilgan tadbirlar orqali namoyon bo'ladi. Ushbu mavzular o'rtasidagi o'zaro ta'sirni tushunish uchun quyidagi jihatlarga e'tibor berish mumkin

Kiberxavfsizlik sohasida shaxsning huquqlari va erkinliklari ehtiyotkorlik bilan himoya qilinishi lozim. Qurbon bo'lgan shaxsning shaxsiy ma'lumotlarini, xususiy hayotini va axborotini himoya qilish kiberxavfsizlikning asosiy maqsadlaridan biri hisoblanadi. Bu borada **ma'lumotning shaxsiyligi** ya'ni internetdagi shaxsiy ma'lumotlarning xavfsizligi va ularning qonuniy tartibda ishlatiladiganligini ta'minlash birinchi galdagi vazifa bo'lsa, **shaxsning shaxsiy hayotini himoya qilish** ya'ni kiberxujumlar orqali shaxsning shaxsiy hayotiga aralashish, xususiy axborotni qonunsiz topish yoki tarqatishning oldini olish keyingi galdagi masala hisoblanadi.

Kiberxavfsizlikning rivojlanishi insonlarning ijtimoiylashuvi bilan chambarchas bog'langan. Internet va raqamli texnologiyalar insonlarning ijtimoiy munosabatlarini yangicha shaklda tashkil etadi. Shaxslar raqamli muhitda ijtimoiy tarmoqlar, forumlar va boshqa onlayn platformada faoliyat ko'rsatadi. Bu munosabatlar, o'z navbatida, kiberxavfsizlikni ta'minotlashga ehtiyojni oshiradi.

Shaxsning ijtimoiylashuvi internet orqali amalga oshirilsa, shaxsiy ma’lumotlar, manzillar, qiziqishlar, yaqinliklar va boshqa ma’lumotlar kiberxujumlarga duch kelishi mumkin. Bu esa shaxslarning ijtimoiy hayotiga xavf soladi.

Ijtimoiy tarmoqlar orqali shaxslar bir-birlari bilan aloqada bo‘lishadi. Ushbu platformalarda ma’lumotlar xavfsizligi, shaxslarning shaxsiyligini himoya qilish va ularning internetdagi xavfsizligini ta’minlash muhim.

Kiberxavfsizlikning huquqiy tomoni ham ahamiyatga ega. Davlatlar va huquqiy tashkilotlar internetdagi xavfsizlikni ta’minlash, shaxslar va tashkilotlarni himoya qilish uchun qonunlarni ishlab chiqadilar. Bu qonunlar shaxsning onlayn huquqlarini himoya qilish, ularning shaxsiy ma’lumotlarini muhofaza qilishga yo‘naltirilgan.

Kiberxavfsizlik shaxsning ijtimoiy hayotiga ta’sir ko‘rsatadi. U internetda ijtimoiy tarmoqlarda faoliyat yuritganida, shaxsning ma’lumotlari, aloqa tarmoqlari va ijtimoiy munosabatlari xavfga tushishi mumkin. Buning oldini olish uchun shaxslarning raqamli xususiyatlari, ya’ni shaxsiy ma’lumotlarini muhofaza qilish, xakerlardan himoya qilish va internetda xavfsizlikni ta’minlash muhim ahamiyatga ega.

Xulosa. **sifatida kiberxavfsizlik** va **shaxs huquqiy ijtimoiylashuvi** bir-biri bilan chambarchas bog‘langan. Kiberxavfsizlik insonning shaxsiy huquqlarini, ma’lumotlarini va internetdagi xavfsizligini himoya qilish uchun muhimdir. Bu, o‘z navbatida, shaxslarning ijtimoiy hayotiga ham ta’sir ko‘rsatadi, ularning internetdagi faoliyatini ishonchli va xavfsiz qilishga yordam beradi.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasi Oliy Majlisi tomonidan 2022 yil 15 aprelda “Kiberxafvsizlik to‘g‘risida” gi O‘zbekiston Respublikasi qonuni.
2. Sotsialnaya pedagogika. Kurs leksiy. Pod. red. M.A.Galaguzovoy. –M.: VLADOS, 2003. –S. 87.
3. Sotsialnыy ensiklopedicheskiy slovar. Na russkom, angliyskom, fransuzskom i cheshskom yazыkax. Redaktor-kordinator – akademik RAN G.V.Osipov –Moskva. Izdatelskaya gruppa infra. m-norma. 1998. –S. 328.
4. Mirziyoyev Sh.M. Konstitutsiya – erkin va farovon hayotimiz, mamlakatimizni yanada taraqqiy ettirishning mustahkam poydevoridir. – T., 2018, 30-bet.

CYBERCRIME AS A TYPE OF FRAUD

*Polytechnic University of Turin, PhD, dotsent **N.E. Makhamatov**,*
*Polytechnic University of Turin, Doctor of Science, Professor **M.S. Yakubov**,*
*Polytechnic University of Turin, basic doctoral student **N.M. Sharifjanova***

Cybercrime is a consequence of the globalization of information and communication technologies and the emergence of international computer networks. Unlike other types of economic crime, cybercrime is currently the fastest growing segment, which is due to the increase in the number of computer users connected to the global Internet, the constant increase in the level of professionalism of cybercriminals, and the sustainable development and improvement of information

technology. Any information and technical innovations significantly expand the scope of cybercrime and create conditions for increasing the effectiveness of hacker attacks.

This is due to the growing number of internet users and the increase in the number of vulnerable devices and systems. Cybercriminals use various methods such as phishing, malware and infrastructure attacks to cause damage and gain access to confidential information.

Here are some statistics that illustrate the rise in cybercrime in recent years:

1. Increase in cyberattacks: Cyberattacks have increased by over 300% in the last five years.

2. Phishing: Phishing incidents account for around 80% of all reported cybersecurity incidents.

3. Ransomware: Ransomware attacks have increased by 435% from 2019 to 2022.

4. Financial losses: The cost of cybercrime to the global economy has increased by 50% in the last three years, reaching over US$6 trillion in 2023.

This type of crime, like all others, poses a threat to the information security of society. In addition to the theft of funds from bank cards.

There are two categories of cybercrimes:

- violent or otherwise potentially dangerous (threat of physical violence, cyberstalking, child pornography, cyberextremism, cyberterrorism);

- non-violent crimes (illegal trespass in cyberspace, cybertheft, cyberfraud, advertising of prostitution services on the Internet, illegal drug trafficking using the Internet, gambling on the Internet, money laundering through electronic movement, destructive cybercrimes and other cybercrimes).

However, in general, cybercrimes are divided into the following types:

- financially-oriented cybercrimes;
- cybercrimes related to invasion of privacy;
- social and politically motivated cybercrimes.

As the number of Internet users grows, the number of cybercriminals also increases, who operate according to one scheme: first, they establish contact with the victim via email or social networks and ask for a response also by email, or by phone, fax or any other means. Once the bait is thrown, the fraudsters try to gain the victim's trust and, eventually, ask for a certain amount of money, using various pretexts.

Phishing is one of the most common types of cyber fraud, based on identifying and extracting personal data from a person to access bank accounts, carried out fraudulently. Most often, hackers send users a file or link containing malicious codes. When such resources are clicked, the data is read, the bank account is hacked and money is withdrawn from it.

Pharming is a type of cybercrime aimed at remotely hacking a computer. Thanks to this, the hacker gets full access to it: he can edit documents, monitor the computer user using audio and video surveillance, introduce various malicious programs, collect information about the user. The main feature of this cybercrime is that the victim will not even guess that at the moment such manipulations are being carried out with his computer.

Cyber drug trafficking is also carried out using information technology. With their help, encrypted coordinates of the location of the goods are communicated to the client, and payment for the «goods» is made.

Cyberterrorism involves the implementation of terrorist acts using and through information technology. Such acts include the dissemination of information about terrorist acts planned for the future, as well as calls for terrorist acts.

The fight against cybercrime is complicated by a number of factors, namely:

- cybercriminals are not ordinary scammers, but well-trained programmers who hide behind their computer screens. It is much more difficult to identify such a person than an ordinary criminal.

- when faced with cybercrime, law enforcement officers need the help of highly qualified specialists in the field of programming, which is still in short supply.

- it is quite difficult to control existing, constantly updated and newly emerging types of cybercrime. In the modern world, cybercrime poses a serious threat to society and its information security.

Cybercrime gives rise to a complex of social problems that require immediate response and effective resolution. With the improvement of information technology, cybercrime is also improving, manifesting itself in many areas of life and activity of a person and society as a whole. Protection from this type of crime involves the correlation of efforts at the level of international cooperation and interaction.

In conclusion, we can highlight some suggestions for improving cybersecurity:

- Updating legislation: Regularly updating legal norms to cover new types of cybercrimes.

- International cooperation: Creating and strengthening international agreements to combat cross-border cybercrimes.

- Creating specialized agencies: Establishing national cybersecurity agencies that will coordinate the efforts of various departments.

- Training and Certification: Conducting regular training and certification to improve the skills of cybersecurity specialists.

- Increasing Investment: Public and private investment in the development of cybersecurity infrastructure.

- Business Stimulation: Providing tax incentives and grants for companies that invest in protecting their information systems.

- Using Modern Technologies: Implementing Artificial Intelligence and Machine Learning to detect and prevent threats.

- Constantly Updating Systems: Regularly updating software and security systems to eliminate vulnerabilities.

- Data Encryption: Using advanced encryption methods to protect confidential information.

- Educational campaigns: Conducting information campaigns to raise public awareness of cyber threats and ways to protect themselves.

- Partnerships with educational institutions: Including cyber security in educational programs and conducting specialized courses.

Implementation of these measures will help to significantly strengthen protection against cyber threats and increase the level of cyber security both at the national and international levels.

LITERATURE

1. Chirkov D.K., Sarkisyan A.Zh. Crime in the sphere of high technologies: trends and prospects // Security issues. 2013. № 2. C.160-181. [Electronic resource]. URL: http://e-notabene.ru/nb/article_608.html (date of access 03.04.2018 г.)
2. Constitution of the Republic of Uzbekistan.
3. Criminal Code of the Republic of Uzbekistan.
4. Decree of the President of the Republic of Uzbekistan «On measures for further improvement of the sphere of information technologies and communications» No. 5349 of 19.02.2018
5. Resolution of the President of the Republic of Uzbekistan “On measures to improve the system of control over the implementation of information technologies and communications, organizing their protection” № 4024 of 21.11.2018.
6. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan "On measures to create a technological park of software products and information technologies" No. 17 of 10.01.2019
7. https://internetpolicy.kg/literacymodule/course_2/module1/glava1_1.html

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ СИЛАМИ НАЦИОНАЛЬНОЙ ГВАРДИИ РЕСПУБЛИКИ УЗБЕКИСТАН

Арпов Ботир Бахтиярович

Начальник цикла Профессианальной подготовки Регионального учебного центра Национальной гвардии Республики Узбекистан

Данный тезис представляет собой всесторонний анализ роли Национальной гвардии Республики Узбекистан в борьбе с киберпреступностью. В нем рассматриваются актуальные проблемы кибербезопасности в Узбекистане, стратегия и тактика Национальной гвардии в противодействии киберугрозам, методы и средства, используемые в работе, а также международное сотрудничество и достижения в этой сфере. Документ также заглядывает в будущее, анализируя перспективы развития и совершенствования системы противодействия киберпреступности в Узбекистане.

Ключевые слова: *национальная гвардия, киберпреступность, противодействие.*

Актуальность проблемы киберпреступности в Узбекистане.

Киберпреступность представляет собой серьезную угрозу для национальной безопасности, экономики и граждан Узбекистана. С развитием информационных технологий и интернета, киберпреступники все чаще используют эти инструменты для совершения различных видов преступлений,

таких как кража личных данных, мошенничество, вымогательство, распространение вредоносных программ, атаки на государственные и коммерческие организации.

В Узбекистане, как и во всем мире, наблюдается рост киберпреступности, что связано с рядом факторов:

- расширение доступа к Интернету и использование мобильных устройств;
- повышение зависимости от информационных технологий в различных сферах жизни;
- недостаток осведомленности и кибергигиены у населения;
- слабая система кибербезопасности в некоторых государственных и коммерческих организациях;

Эти факторы создают благоприятную почву для деятельности киберпреступников, что требует принятия эффективных мер по противодействию киберугрозам.

Роль национальной гвардии в обеспечении кибербезопасности

Национальная гвардия Республики Узбекистан играет важную роль в обеспечении кибербезопасности страны. Она является одним из ключевых органов, ответственных за защиту информационной инфраструктуры государства, борьбу с киберпреступностью и предотвращение кибератак.

Основные функции Национальной гвардии в этой области включают:

- мониторинг и анализ киберугроз;
- проведение расследований киберпреступлений;
- предотвращение и пресечение кибератак на государственные и коммерческие организации;
- обучение и подготовка специалистов по кибербезопасности;
- сотрудничество с другими правоохранительными органами и международными организациями в борьбе с киберпреступностью.

Национальная гвардия обладает необходимыми ресурсами и опытом для эффективного выполнения этих задач. Ее сотрудники проходят специализированную подготовку по кибербезопасности и владеют современными методами и инструментами для противодействия киберугрозам.

Стратегия и тактика национальной гвардии в борьбе с киберугрозами.

Национальная гвардия использует комплексный подход к борьбе с киберугрозами, который включает в себя следующие ключевые элементы:

Профилактика: повышение осведомленности населения о кибербезопасности, обучение основам кибергигиены, проведение информационных кампаний по защите от киберпреступности.

Превентивные меры: усиление защиты информационной инфраструктуры государства и коммерческих организаций, внедрение современных систем кибербезопасности, проведение регулярных аудитов безопасности.

Активные действия: выявление и пресечение кибератак, проведение расследований киберпреступлений, задержание и привлечение к ответственности киберпреступников.

Сотрудничество: взаимодействие с другими правоохранительными органами, международными организациями, частными компаниями, занимающимися кибербезопасностью.

Тактика Национальной гвардии в борьбе с киберугрозами адаптируется к изменяющимся угрозам и включает в себя использование различных методов и средств, таких как:

Сбор и анализ данных: использование специализированных инструментов и технологий для сбора и анализа информации о киберугрозах, идентификации источников атак и выявления мотивов киберпреступников.

Кибербразведка: проведение оперативноQрозыскных мероприятий, направленных на выявление и нейтрализацию киберпреступников, а также их ресурсов и инфраструктуры.

Проведение кибероперацій: применение специализированных средств и методов для пресечения кибератак, восстановления поврежденных систем, ограничения доступа к зараженным ресурсам.

Правовое преследование: доказательство вины киберпреступников, их задержание и привлечение к ответственности в соответствии с законодательством Узбекистана.

Методы и средства, используемые национальной гвардией

Национальная гвардия использует широкий спектр методов и средств для противодействия киберпреступности, включая:

Технический анализ Использование специализированных программных инструментов для анализа данных, выявления вредоносных программ, анализа трафика, идентификации сетевых атак.

Для анализа данных используются такие средства, как SIEMQ системы MSecurity Information and Event ManagementN, анализаторы сетевого трафика, системы детектирования интрузий MIDSN, программы для анализа вредоносного кода.

Оперативно-розыскные мероприятия Проведение оперативно-розыскных мероприятий, направленных на выявление и нейтрализацию киберпреступников, а также их ресурсов и инфраструктуры.

Специалисты Национальной гвардии используют методы тайного контроля, опроса, наблюдения, в том числе с применением специальных технических средств.

Правовое преследование Сбор доказательств киберпреступлений, подготовка материалов для уголовного дела, участие в процессе задержания и привлечения к ответственности киберпреступников.

Специалисты Национальной гвардии тесно сотрудничают с прокуратурой, судами и другими правоохранительными органами в рамках правового преследования киберпреступников.

Взаимодействие Национальной гвардии с другими правоохранительными органами.

Национальная гвардия активно сотрудничает с другими правоохранительными органами Узбекистана в борьбе с киберпреступностью.

Это сотрудничество является ключевым элементом эффективного противодействия киберугрозам и основано на следующих принципах:

1 **Обмен информацией** Регулярный обмен данными о киберугрозах, киберпреступниках, методах и средствах, используемых для совершения киберпреступлений.

2 **Совместные операции** Проведение совместных оперативно-розыскных мероприятий по пресечению кибератак, задержанию и привлечению к ответственности киберпреступников.

3 **Согласование действий** Согласование стратегий и тактики противодействия киберпреступности, определение ролей и ответственности каждого правоохранительного органа.

Важное место в системе взаимодействия занимают сотрудничество с Министерством внутренних дел, Службой государственной безопасности, Прокуратурой и другими органами, отвечающими за обеспечение правопорядка и безопасности в стране.

Подготовка и обучение личного состава национальной гвардии.

Национальная гвардия уделяет особое внимание подготовке и обучению своего личного состава в области кибербезопасности. Программы обучения охватывают широкий спектр тем, включая:

- основы кибербезопасности;
- методы и средства противодействия киберугрозам;
- анализ киберугроз и инцидентов;
- проведение кибероперации;
- правовые аспекты кибербезопасности;
- сотрудничество с международными организациями.

Обучение личного состава проводится в специализированных учебных центрах Национальной гвардии, а также с привлечением специалистов из других правоохранительных органов, коммерческих компаний и международных организаций.

Регулярное повышение квалификации личного состава Национальной гвардии позволяет обеспечить высокий уровень подготовки специалистов и эффективное противодействие киберугрозам.

Международное сотрудничество в области противодействия киберпреступности.

Национальная гвардия активно развивает международное сотрудничество в области противодействия киберпреступности. Это сотрудничество необходимо для обмена опытом, информацией и технологиями, а также для координации действий в борьбе с транснациональной киберпреступностью.

Национальная гвардия участвует в работе международных организаций, занимающихся противодействием киберпреступности, таких как Интерпол, Европол, Организация Объединенных Наций. Она также поддерживает тесные контакты с правоохранительными органами других стран и обменивается опытом с ними.

Международное сотрудничество позволяет Национальной гвардии получить доступ к новейшим технологиям и методам противодействия

киберпреступности, а также укрепить международные связи в борьбе с транснациональными киберугрозами.

Достижения и успехи Национальной гвардии в борьбе с киберугрозами.

Национальная гвардия добилась значительных успехов в борьбе с киберугрозами в Узбекистане. За последние годы она провела ряд успешных операций по пресечению кибератак, задержанию и привлечению к ответственности киберпреступников.

Среди ключевых достижений Национальной гвардии можно выделить:

- пресечение ряда кибератак на государственные и коммерческие организации;
- задержание и привлечение к ответственности многих киберпреступников;
- разработка и внедрение новых методов и средств противодействия киберугрозам;
- повышение осведомленности населения о кибербезопасности;
- укрепление международного сотрудничества в области противодействия киберпреступности.

Эти достижения свидетельствуют о высоком профессионализме и эффективности работников Национальной гвардии, а также о важности ее роли в обеспечении кибербезопасности Узбекистана.

Перспективы развития и совершенствования системы противодействия киберпреступности.

В будущем противодействие киберпреступности будет оставаться важным приоритетом для Национальной гвардии. Для успешной борьбы с киберугрозами необходимо продолжать совершенствовать систему противодействия киберпреступности, укреплять ее ресурсы и технологии, а также развивать международное сотрудничество.

К ключевым направлениям развития системы противодействия киберпреступности в Узбекистане можно отнести:

- укрепление законодательной базы в области кибербезопасности, уточнение и расширение правовых норм для эффективного пресечения киберпреступлений;
- развитие систем кибербезопасности, внедрение современных технологий, таких как искусственный интеллект, машинное обучение, блокчейн для автоматизации процессов выявления и пресечения киберугроз;
- повышение осведомленности населения о кибербезопасности с помощью проведения информационных кампаний, обучения в школах и вузах, разработки программ повышения кибергигиены;
- развитие международного сотрудничества в области противодействия киберпреступности с целью обмена опытом, информацией и технологиями, а также координации действий в борьбе с транснациональной киберпреступностью.

Вывод. Сочетание всех этих направлений позволит Узбекистану создать прочную систему противодействия киберпреступности, способную обеспечить надежную защиту национальных интересов от киберугроз.

Список литературы

1. Ю. Гаврилов. Технические средства охраны: Учебное пособие. М.: 12 Главное управление Министерства обороны Российской Федерации, 2010. 58 с.
2. Официальный сайт Правительственный портал Республики Узбекистан [Электронный ресурс]. – gov.uz: https://www.gov.uz/

KIBERJINOYATCHILIKNING IJTIMOIY VA IQTISODIY XAVFI

Muxtorov Jo‘rabek Sayidqulovich

O‘zbekiston Respublikasi IIV Malaka oshirish instituti yuridik fanlar kafedrasi professori, yu.f.n., professor

Annotatsiya: kiberjinoyatchilikning tushunchasi, ijtimoiy va iqtisodiy xavfi, tahdidlar, davlat organlari, tashkilotlar va fuqarolarga yetkazayotgan zararlari ko‘lami, mazkur jinoyatning oldini olishga doir chora tadbirlar ilmiy asoslangan holda yortib berilgan.

Kalit so‘zlar: kiberjinoyatchilik, xakerlar, dasturiy ta’minot va texnik vositalar, axborot tizimlari va resurslari, shaxsiy ma’lumotlar, kiberhujumlar.

Shiddat bilan rivojlanib borayotgan fan va texnika sohasidagi yutuqlari kundalik ijtimoiy hayotimizga yanada qulay shart-sharoit hamda imkoniyatlarni taqdim etmoqda. Biroq, ana shu qulayliklar va afzalliklar bilan bir qatorda, mazkur texnika yutuqlaridan ayrim shaxslar o‘z manfaatlari yo‘lida noto‘g‘ri foydalanishlari hamda o‘zga shaxslarga ijtimoiy va iqtisodiy zarar yetkazmoqdalar.

Achinarlisi, bunday holatlarning kundan kunga ko‘payotganligi, buning natijasida ko‘plab insonlar ham ijtimoiy ham iqtisoiy zarar ko‘rayotganligi, kerak bo‘lsa o‘lim bilan bog‘liq holatlar ham kuzatilayotganligi mazkur masalaning naqadar dolzarb ekanligini ko‘rsatadi. Bizningcha, mazkur masala butun dunyo muammosiga aylandi desak hato qilmagan bo‘lamiz. Shulardan biri kiberjinoyatchilikdir.

Kiberjinoyatchilik – axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisidir[11]. Kiberjinoyatchilik – bu kompyuter, kompyuter tarmog‘i yoki tarmoq qurilmasidan suiiste’mol qilishga qaratilgan jinoiy faoliyat hisoblanadi. Ularning aksariyati kiberjinoyatchilar yoki xakerlar tomonidan undan noqonuniy daromad orttirish maqsadida sodir etiladi. Bu esa, o‘z navbatida, barchamizni tashvishga solishi va bu muammoning yechimini topishga undashi aniq.

Binobarin, mazkur jinoyat respublikamizda ham sodir etilayotgani va fuqarolarimiz ushbu jinoyatdan jabrlanayotgani kuzatilmoqda. Xususan, odamlar kartochkalaridan pulni o‘marish sezilarli darajada oshdi. Firibgarlik jinoyatlari soni

[11] O‘zbekiston Respublikasining 2022 yil 15 apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida” qonuni.

ham oshib borayotgani barchamiz uchun xavotirlidir. Holbuki, barcha toifadagi shaxslar ham firibgarlarning tuzog‘iga tushmaslikdan kafolatlanmagan. Boz ustiga texnologiya rivoj topgani sari firibgarlikning yangidan yangi turlari, ularning yangi tuzoqlari va aldov yo‘llari paydo bo‘lmoqda.

Ma’lumki, huquqni muhofaza qiluvchi organlar tomonidan bu jinoyatchilar aniqlanib, jinoyatchilarga nisbatan tegishli jazo choralari ko‘rilmoqda va jarblanuvchilarga zararlar undirib berilmoqda.

Biroq, shunga qaramay zamonaviy dunyoda kiber tahdidlar soni tez sur’atlar bilan o‘sib bormoqda. Xakerlar oddiy fuqarolarning bank hisoblarini bo‘shatishmoqda, shuning uchun ham bugungi xayotimizda raqamli dunyo tahdidlaridan ishonchli himoya asosiy ehtiyojga aylanib bormoqda. Mazkur sohada izlanishlar olib borayotgan ekspertlarning fikricha, bir yilda kiberjinoyatlarning global zarari bir necha trillion dollarga etishi mumkin ekan.

Aksariyat kiberhujumlar, kiberjinoyatchilar yoki xakerlar tomonidan og‘ir mehnat qilmasdan engil pul topish, ishlamasdan moliyaviy daromad olish maqsadida amalga oshiriladi. Bu esa o‘z navbatida davlatlar va fuqarolarga iqtisodiy zarar yetkazadi. Biroq, kiberhujumlarning maqsadi shaxsiy yoki siyosiy sabablarga ko‘ra kompyuterlar yoki tarmoqlarni o‘chirish ham bo‘lishi mumkin. Tadqiqotlardan ma’lumki, kiberjinoyatlar yangi boshlanuvchi xakerlardan tortib ilg‘or texnikadan foydalanadigan va texnologiyani yaxshi biladigan jinoiy guruhlargacha bo‘lgan shaxslar va tashkilotlar tomonidan sodir etilmoqda.

Shuni alohida ta’kidlash joizki, yuqorida aytganimizdek oson kelgan boylik xakerlikni avj oldirmoqda. Ayni paytda viruslar orqali amalga oshirilayotgan kiberhujumlar juda xatarli tus olmoqda. Tarqatilayotgan viruslarning aksariyati bank xizmatlarini ko‘rsatadigan jahon axborot tarmog‘ini zaiflashtirish orqali, u yerdan moliyaviy ma’lumotlarni o‘g‘irlashni ko‘zlagan. Tahlillaridan ma’lum bo‘lishicha, bank-moliya sohasidagi yirik muassasalar, onlayn to‘lov jarayonlarini amalga oshiruvchi tizimlar, savdo majmualari, mehmonxona va savdo terminallari eng ko‘p foydalaniladigan markazlar xakerlarning asosiy diqqat markazida bo‘lgan.

Jumladan, odamlarga bank xizmatlarini ko‘rsatishni taklif qilish, soxta bank tizimlarini yaratish orqali zarur axborotlarni o‘g‘irlash, elektron pochtalar orqali bank tizimlariga hujum uyushtirish, internet tarmog‘ida turli xildagi qiziqarli aksiya va viktorinalarni tashkil etish orqali foydalanuvchilarning ma’lumotlarini o‘g‘irlash holatlari kuzatilmoqda.

Shuning bilan birga bugungi kundagi kuchli raqobat – xakerlik rivojiga xizmat qilmoqda. So‘nggi yillarda xakerlarning veb-saytlarga uyushtirayotgan hujumlari soni tobora oshib borayotgani kuzatilgan. O‘tgan asrning 60-yillarida “xaker” so‘zi kompyuter va axborot texnologiyalarini puxta bilgan insonlarga nisbatan ishlatilgan. Bugungi kunga kelib esa, bu so‘z axborot-kommunikatsiya texnologiyalari yordamida noqonuniy harakatlarni bajaruvchi, axborot tizimlari va dasturlarini buzib kirib, ulardan ruxsatsiz foydalanuvchi, ilova hamda veb-sahifalar muhofazasini buzish va virus tarqatish orqali kiber jinoyatchilik qiladigan shaxsga nisbatan aytiladi.

Bugungi kunda kiberjinoyatning ijtimoiy xavfini quyidagilarda ko‘rishimiz mumkin:

- muayyan shaxsning yoki ob’ektning geografik joylashgan nuqtasi to‘g‘risida xabar tarqatish, shaxsiy ma’lumotlar bazasini buzib kirishda. Xakkerlar bu kabi ma’lumotlarni internet va ijtimoiy tarmoq foydalanuvchilari tomonidan turli elektron resurslarga ularning foydalanish shartlarini o‘qimasdan turib kirishlari evaziga olishmoqda;

- internetga ulangan avtomobil va uylarning xavfsizligi bilan bog‘liq muammolar. Internetga ulangan har qanday gadjetning IP-manzili orqali “aqlli uy”larning holati to‘g‘risida ma’lumotlarni o‘g‘irlash, kompyuterlar tarmog‘i bo‘lgan botnetlarga hujum uyushtirish shuningdek, internetga ulangan deyarli barcha avtomobillarning raqamli kalitlarini tayyorlash va tizimlarini masofadan boshqarish mumkin;

- xakerlar nafaqat videokameralar, avtomobil, samolyot kompyuterlari, balki bugun ommalashyotgan “aqlli chiroq”larni, bundan ham jiddiyroq xavfsizlik tizimlarini masofadan turib ishdan chiqarishadi va ularning ustidan nazoratni qo‘lga olishadi. Natijada, ular yirik avariya, yong‘in va boshqa turdagi baxtsiz hodisalarni sun’iy ravishda keltirib chiqarishadi;

- xakerlar atom stansiyalariga ham xujum uyushtirishi mumkinligi, bu esa fojeali texnogen halokatlarni keltirib chiqarishidan dalolat beradi.

Shuning bilan birga, “statistik ma’lumotlarga ko‘ra, dunyo yoshlarining 96 foizi ijtimoiy tarmoqlar vositasida o‘zaro muloqotga kirishmoqda. Muloqotlar ko‘pincha kiberjinoyatchilar uchun juda qulay sharoit ekanligini har bir yosh bilmog‘i lozim. Vertual tarmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish, xakkerlik hujumi veb-saytlarga noqonuniy kirish, firibgarlik, mualliflik huquqini buzish, kredit kartochkalari raqami va bank rekvizitlarini o‘g‘irlash, shaxsiy ma’lumotlar, surat va videolarni o‘g‘irlab, ularni tarqatib yuborish tahdidi bilan odamlarni shantaj qilib, pul talab qilishlari ham mumkin. Siz kimsiz, qaysi mamlakatda yashaysiz – xakkerlar uchun buning ahamiyati yo‘q. Kompyuterdan foydalanyapsizmi, demak ular sizni istagan payt nishonga olishi mumkin”[12].

Bundan tashqari, tarmoq pedagogik nuqtai nazardan quyidagi xavfli ta’sirlarga ham ega:

1) internet tarmog‘iga bog‘lanib qolish;

2) o‘qish va bilim olishga yengiltaklik bilan munosabatda bo‘lish. Internetdan tayyor dars ishlanmalari, matematik masalalar yechimlarini osongina topish hisobiga dars topshiriqlarini mustaqil bajarmaslik;

3) jismoniy rivojlanishiga salbiy ta’sir xavfi, ya’ni bolaning faol harakatda bo‘lmay, uzoq vaqt monitor ro‘parasida o‘tirishiga to‘g‘ri kelishi va boshqalar[13].

Kiberjinoyatchilikning oldini olish maqsadida quyidagi chora-tadbirlarni amalga oshirish maqsadga muvofiq:

1. Himoyalangan kuchli platforma yaratish;

---

[12] Qarang: *Subanov O.S.* Kibberterrorizm hamda axborot xurujlaridan yoshlarimizni himoya qilishda ichki ishlar organlarining asosiy vazifalari/ Axborot texnologiyalar orqali sodir etilayotgan jinoyatlarga qarshi kurashishning dolzarb muammolari. Respublika ilmiy-amaliy konferensiya to‘plami (2023 yil 18 may). – T.: O‘zbekiston Respublikasi IIV Malaka oshirish instituti. 2023. – 233-b

[13] O‘sha manbaa.

2. Kuchli parollar o‘rnatish;

3. Xodimlar (mutaxassislar)ni zamoanaviy bilimlar yangiliklar asosida o‘qitish;

4. Ma’lumotlarni muntazam nazorat qilib borish;

5. Ma’lumotlarni shifrlash tizimlarini takomillashtirish.

Yurtimizda kiberjinoyatchilikka qarshi kurash tizimini takomillashtirish maqsadida O‘zbekiston Respublikasi Prezidentining 2022 yil 28 yanvardagi “2022 – 2026 yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi PF-60-son Farmonining 89-maqsadida “Kiberjinoyatchilikning oldini olish tizimini yaratish” kabi ustuvor vazifa belgilab berildi. Bu Farmonning 2-ilovasida esa “Tergov faoliyati ustidan samarali nazorat o‘rnatish, axborot texnologiyalari yordamida sodir etilayotgan jinoyatlarga qarshi kurashishda tezkor-qidiruv faoliyatini yanada kuchaytirish” hamda “Kiberjinoyatchilikning oldini olish tizimini yaratish” ustuvor yo‘nalishlar, maqsadlar va vazifalarni o‘z ichiga olgan davlat dasturi tasdiqlanib amaliyotga tatbiq etildi.

Kiberjinoyatchilikka qarshi kurashda xavfsizlik choralarini ko‘rish bo‘yicha vakolatli huquq-tartibot hamda bank idoralari bilan hamkorlikda muayyan chora-tadbirlar amalga oshirib kelinmoqda. Bilamizki, internet tarmog‘ida shubhali manbalar orqali ma’lumot olish, norasmiy ilovalarni yuklab olish, e’lon va elektron manzillarga javob berish imkoniyati cheklab qo‘yilgan.

Jumladan, shubhali va ishonchsiz manbalar bilan bog‘lanish natijasida nafaqat ma’lumotingiz tarqalib ketishi, balki pullaringizdan ayrilib qolish xavfi borligini doimo yodda tutish zarur.

Xususan, jinoyatchilar telefon apparati va internet tarmog‘i orqali boshqa davlatlarda ro‘yxatga olingan telefon raqamiga “Telegram” ijtimoiy tarmog‘ida tegishli akkauntlarni ro‘yxatga olib, mazkur tashkilotlar nomidan “Telegram” ijtimoiy tarmog‘ida guruh obunachilarining ishonchiga kirib, aldov yo‘li bilan ularga tegishli bo‘lgan bank plastik kartalarining barcha mablag‘ini internet tarmog‘i orqali xalqaro pul o‘tkazmalar tizimiga ulanib yechib olmoqda. Jinoiy yo‘l bilan topilgan mablag‘larni internet tarmog‘i orqali legallashtirib, boshqalar nomiga bank tomonidan rasmiylashtirilgan Virtual bank plastik kartasiga o‘tkazib yuborayotgani ma’lum bo‘lmoqda.

Shu bois fuqarolarimizga bu borada ham tushuntirish va targ‘ibot ishlari olib borilmoqda. Jumladan, fuqarolarimizning shunga o‘xshash firibgarlik hamda o‘g‘rilik holatlariga duchor bo‘lmasliklari uchun o‘zlarining sir saqlanishi lozim bo‘lgan plastik kartalari raqamini oshkor etmasligi, birovga rasmga tushirib bermasligi yoki og‘zaki tarzda ma’lum qilmasliklari to‘g‘risida tushuntirishlar berilmoqda.

Adabiyotlar ro‘yxati:

1. Sh.M.Mirziyoev. Milliy taraqqiyot yo‘limizni qatiyat bilan davom ettirib, yangi bosqichga ko‘taramiz. T.1.–T: “O‘zbekiston” NMIU, 2018., 591-b.
2. Mirziyoev Sh.M. Xalqimzning roziligi bizning faoliyatimizga berilgan eng oliy bahodir.- Toshkent - «O‘zbekiston»,- 2018. – 512 b.
3. Konstitutsiya – erkin va farovon hayotimiz, mamlakatimizni yanada taraqqiy ettirishning mustahkam poydevoridir / Prezident Shavkat Mirziyoevning O‘zbekiston

Respublikasi Konstitutsiyasi qabul qilinganining 25 yilligiga bag‘ishlangan tantanali marosimdagi ma’ruzasi // URL: http://xs.uz (Xalq so‘zi, 08.12.2017).
4. Axborot texnologiyalar orqali sodir etilayotgan jinoyatlarga qarshi kurashishning dolzarb muammolari. Respublika ilmiy-amaliy konferensiya to‘plami (2023 yil 18 may). – T.: O‘zbekiston Respublikasi IIV Malaka oshirish instituti. 2023. – 256-b
5. O‘zbekiston Respublikasining 2022 yil 15 apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida” qonuni.
6. B.Umarov, M.Axmedova. Ochiq axborot tizimlarida axborot-psixologik xavfsizlik. – T.: - 2012.
7. L.S .Tursunov. Psixologik xavfsizlik asoslari. – T.: - 2012.
8. Ma’naviyatimizga tahdid – kelajakka tahdid. Ilmiy-maqolalar to‘plami. Respublika Ma’naviyat va ma’rifat kengashi respublika ma’naviyat targ‘ibot markazi. Toshkent, 2011. 199-b.
9. Demokratlashtirish va inson huquqlari. Ilmiy-ma’rifiy jurnal. 2021 yil 1-son., 167-b.
10. Sh.Odilxonovna. “Ommaviy madaniyat” tahdidi. –T., “Muharrir nashriyoti” – 2010. 18-b.
11. Diniy ekstremizm va terrorizmga qarshi kurashning ma’naviy-ma’rifiy asoslari. Mas’ul muharrir: Z.Islomov. – T.: Toshkent islom universiteti, - 2017. – 246-b.

MUHIM AXBOROT INFRATUZILMALARINI YASHIRIN HID INTERFEYSLI USB QURILMALARIDAN KIBERHIMOYALASH

AXMETOV Rustam Dilshatovich

O‘zbekiston Respublikasi Qurolli Kuchlari Akademiyasi Ichki ishlar vazirligi qo‘shinlarini tayyorlash kafedrasi o‘qituvchi

Jismoniy zarar etkazishga qodir birinchi kiberqurol.

Muhim axborot infratuzilmalariga maqsadli ravishda kiberhujumni amalga oshirish uchun USB tizimi zaifligidan foydalanib, yaratilgan **zararli USB qurilma** jismoniy zarar yetkazishga qodir **BIRINCHI KIBERQUROL sifatida** tarixiga kirgan.

Bunday kiber qurol yordamida Erondagi uranni qayta ishlash dasturiga nisbatan **Stuxnet** kiberhujumi amalga oshirilgan va infratuzilmani boshqaruv va nazorat qilish tizimi qo‘lga olingan hamda 5000 ga yaqin sentrafugalarni zararlashga erishilgan.

Dunyoda jumladan mamlakatimizda ham bu kabi kiberhujumlarning soni ko‘payib bormoqda. IIV Kiberxavfsizlik Markazi bergan ma’lumotlarga tayanadigan bo‘lsam,

2021-yilda Xorazmdagi bank xodimi tomonidan kompyuteriga o‘zi bilmagan holda zararli USB qurilmani ulangan va u orqali amalga oshirilgan kiberhujum natijasida **1 milliard** dollardan ortiq mablag‘ boshqa hisob raqamlarga yo‘naltirilgan. 2023-yilda IIV ga fuqaro va tashkilotlar tomonidan USB qurilmalar bilan bog‘liq kiberjinoyatlar bo‘yicha jami 1000 dan ortiq murojaatlar kelib tushgan.

Bugungi kunda kiberhujumlarni o‘ta destruktiv turlarining ko‘payib borishi va xakerlarning nishoni muhim ahborot infratuzilmalariga qaratilayotgani ushbu yo‘nalishda kiberhimoyani ta’minlash dolzarbligini oshirmoqda.

“Axborot-kommunikatsiya texnologiyalari sohasi qanchalik rivoj topgani sari, uning afzalligi va qulayliklaridan foydalanish bilan bir qatorda, butun mamlakatimizda axborot xavfsizligini ta’minlash eng dolzarb masalaga aylanib bormoqda.”

O‘zbekiston Respublikasi Qurolli Kuchlar Oliy Bosh Qo‘mondoni Sh. M. Mirziyoev

Bugungi kunda mamlakatimizda muhim ahborot infratuzilmalarining kiberxavfsizligini ta’minlashga katta etibor qaratilmoqda:

O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi qabul qilinga Qonuni;

O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar” to‘g‘risidagi PQ-167-son Qarori.

Kiberhujumlarni amalga oshirish uchun aynan USB fleshka bo‘lishi shart emas. Ushbu slaydda ko‘rsatib o‘tilgan istalgan qurilmaga reverse engenering qo‘llab uni KIBERQUROL ga aylantirish mumkin.

USB zaifliklaridan foydalanuvchi hujum usullari va turlari tahlili.

Pog‘ona	Hujum usuli	Hujum turi	Himoyalanish vositalari
Inson pog‘onasi	Ijtimoiy muhandislik	Maxsus qurilmalarni tashlab qo‘yish.	Begona USB qurilmalarni kompyuterga ulamaslik va kompyuterda USB portlarni yopib qo‘yish
	Noto‘g‘ri xatti xarakatlar (xatolar)	Qurilmani yo‘qotib yoki o‘g‘irlatib qo‘yish.	Qurilmadagi va ichki tizimdagi barcha ma’lumotlarni shifrlash
Dasturiy ta’minot pog‘onasi	Kodni kiritish	Stuxnet, Duqu, Con-ficker va Flame zararli dasturlari.	Antivirus, DLP, IPS/IDS tizimlari
	Ma’lumotlarni o‘g‘irlash	Web-kamera, USBee.	
	Zararli paketlar	FaseDancer, Debugger, syzkaller.	
Mantiqiy pog‘ona	Yashirin interfeyslar	Rubbery Ducky, USBdriveby, PHUKD/URFUKED, TURNIPSCHOOL, CottonMouth, USBHarpoon, O.MG Cable, Vapinator, Bush Bunny, Spyduino, BadUSB.	**Himoya vositalari yetarli darajada emas**
Interfeys pog‘onasi	Signallarni egallab olish	KeyGrabber, Air Drive Forensic Keylogger, JitterBug, Crosstalk Leakage, USBproxy.	**Himoya vositalari yetarli darajada emas**
	Fizik jihatdan zarar berish	USB Killer	

Ilmiy tadqiqotlar davomida USB tizimining zaifliklaridan foydalanib amalga oshiriladigan kiberhujumlarni o‘rganib chiqildi va tahlil natijalari ushbu jadvalga keltirilgan.

Tahlil natijalari **Mantiqiy** va **interfeys** pog‘onolaridagi zaifliklardan kiberhimoyani ta’minlovchi vositalarning samarasi yetarli darajada emasligi aniqlandi.

Ilmiy tadqiqotlar **USB mantiqiy pog‘onadagi zaifliklardan** kiberhimoyani ta’minlash yo‘nalishida olib borishni belgilab oldi.

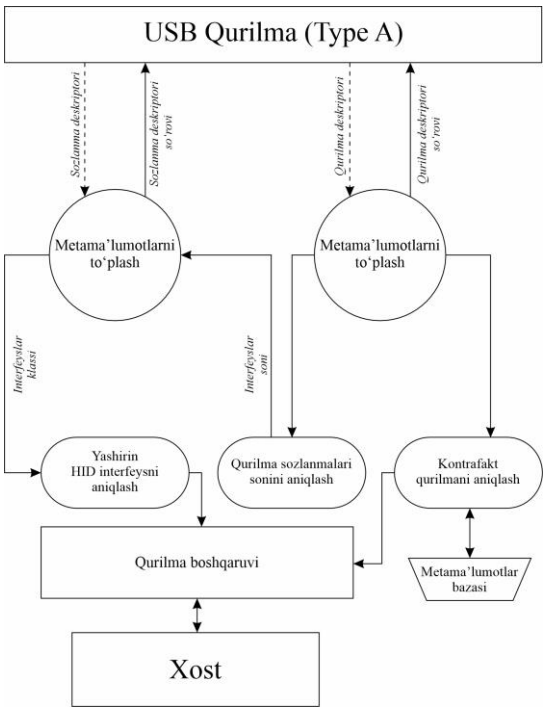
Mantiqiy pog‘ona zaifliklaridan kiberhimoyani ta’minlovchi mavjud usul va vositalarning tahlili.

Vosita turi	**Vositaning nomlanishi**	**Himoya usuli**	**Mavjud usul va vositalarning imkoniyatlari**							
			Dasturiy ta’minot pog’onasida ishlashi	Mantiqiy pog‘onada ishlashi	Interfeys pog‘onasida ishlashi	Avtonom holda ishlashi	USB qurilma boshqaruvini amalga oshirish	Fizik hujumlardan himoyalash	**Yashirin HID Interfeyslarni aniqlash**	**Vendor tekshiruvini amalga oshirish**
Dasturiy vosita	IronKey, FirmUSB, Viper	Firmware verification	✓	–	–	–	–	–	–	–
	Syzkaller, POTUS, vUSBf	USB stack fuzzing	✓	–	–	–	–	–	–	–
	USBFILTER/usbtables, USB Firewall	USB Firewall	✓	✓	–	–	✓	–	–	–
	GoodUSB, Cinch	Host-Emulating Honeypots	✓	–	–	–	✓	–	–	–
Apparat vosita	Secure Xchange USB	Nomalum	–	–	–	✓	✓	✓	–	–
	Armadillo, USG v1.0	Nomalum	–	–	–	✓	✓	✓	–	–

USB mantiqiy pog‘onasi zaifliklaridan kiberhimoyani ta’milashga qaratilgan dunyodagi mavjud vostilarni o‘rganib chiqib va imkoniyatlarini 8 ta mezon bo‘yicha tahlil qilindi. Tahlil natijalari jadvalga keltirilgan.

USB mantiqiy pog‘onasidagi zaifliklaridan himoyalashdagi mavjud muammo va kamchiliklardan kelib chiqib kiberhimoyalanishning yangi usul va algoritmlarini ishlab chiqishni taqazo qildi va bulardan biri.

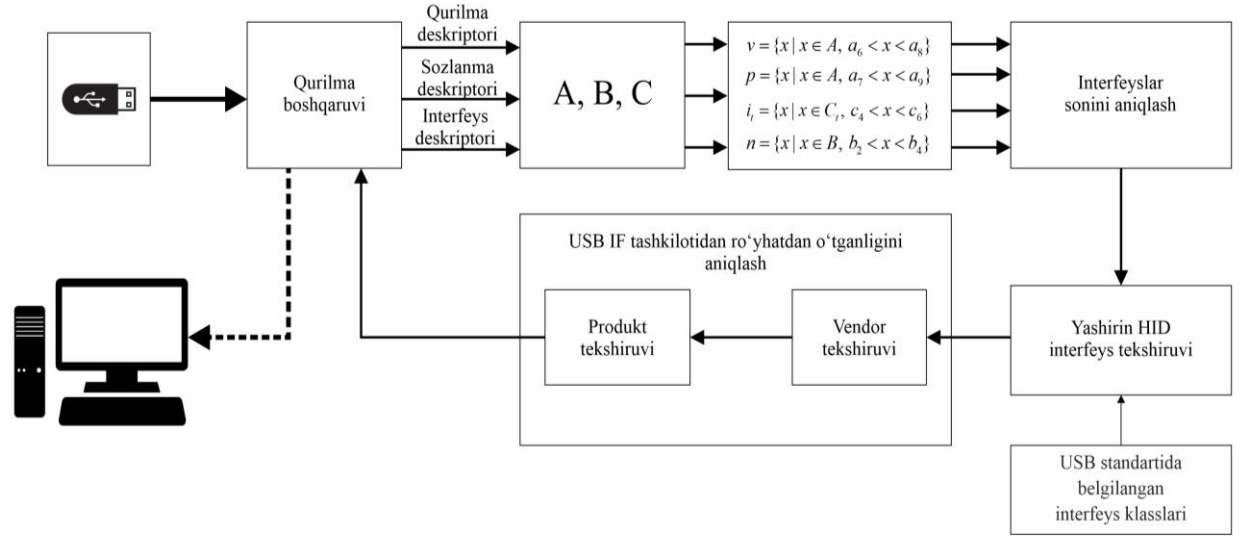
USB qurilmani metama’lumotlari asosida identifikatsiyalash usuli



Tizimga ulanayotgan qurilmalarini identifikatsiya qilishda USB metama'lumotlaridan foydalanish hisobiga avtomatik identifikatsiya usuli takomillashtirildi.

Takomillashtirilgan avtomatik identifikatsiyalash usulida, USB qurilmaning vendor (VID), mahsuloti (PID), interfeyslar soni va klassiga tegishli metama'lumotlarni qayta ishlash nazarda tutilgan.

USB metama'lumotlarini qayta ishlash modeli



Takomillashgan avtomatik identifikatsiyalash usuli asosida **USB metama'lumotlarini qayta ishlash modelini ishlab chiqdi.**

Yangi ishlab chiqilgan modelda:

- USB metama'lumotlarni to'plash va saralash, saralangan metama'lumolar asosida;
- interfeyslar sonini aniqlash, yashirin HID interfeys va vendor, mahsulot tekshiruvi natijalari asosida.

USB qurilma boshqaruvini amalga oshirish belgilangan.

ВОЯГА ЕТМАГАН ШАХСЛАР ТАРБИЯСИДА АХБОРИЙ-ПСИХОЛОГИЯ ВА ТАРБИЯНИНГ ЎРНИ

Ғозибеков Тўлқин Ҳабибуллаевич

ИИВ Малака ошириш институти Махсус касбий фанлар кафедраси доценти

Аннотация: Мазкур мақолада глобаллашув шароитида Вояга етмаган шахслар онгига салбий таъсир кўрсатувчи, интернет омиллар ва уларнинг олдини олиш юзасидан тавсиялар келтирилган, ахборий-психологик хавфсизлиги билан боғлиқ бўлган фаолияти илгари сурилган.

Калит сўзлар: кибир жиноятчилик, ахборий-психология ва хавфсизлик, вояга етмаган шахслар сиёсати, интернет, виртуал олам, ижтимоий тармоқлар, манипулятсия, ассертивлик, мафкуравий иммунитет.

Бугунги кунда шиддат билан ривожланаётган даврда фарзандларимизни ақлан, рухан, жисмонан бақувват ва соғлом бўлишларини таъминлашнинг ўзи етарли бўлмайди. Балки, бу даврда бизни болаларимиз замонга хос ва мос юксак маърифатли, бунёдкор, шижоатли бардавом баркамол авлод этиб, тарбиялаш ва тайёрлаш зарурати ҳар-биримизни ҳамда таълим муассасалари олдига қўйилган катта масъулят деб ҳисоблаймиз.

Муҳтарам, Президентимиз ўз табирларида “Биз оилани ҳаёт давомийлигини таъминлайдиган, буюк келажак авлод тақдирига кучли таъсир кўрсатадиган тарбия маскани сифатида қабул қиламиз.[14] ”. Зеро, боланинг келажаги ушбу масканда қандай тарбия олганлиги, унинг тарбиясида ота-онанинг ўз бурч ва вазифаларига қандай ёндашганига боғлиқдир деган сўзлари биз учун дастури амал бўлиши керак.

Оилада инсон, энг аввало, соғ-омон вояга етади, яхши хулқ наъмуналарини ўзлаштиради, ўзида мақсадга мувофиқ шахслараро муносабатлар кўникмаларини шакллантиради. Бунда ота-онанинг ўрни катта бўлади. Ҳар бир ота-она ўз фарзандини таълим жараёнида ва таълимдан сўнг имкон қадар назорат қилиши, унга 10 та лелефон эмас битта бўлсада ватан тараққиёти йўлидаги эзгу китоб олиб бериши ва ҳунар ўргатиши бугунги куннинг долзарб масаласига айланган.

Халқимизда қуш инида кўрганини қилар деб бежиз айтишмаган. Бугунги кунда кўплаб ҳуқуқбузарликлар айнан телефон, телеграм ва истаграм ҳамда вайбер тармоқлари орқали содир этилаётганлиги барчага маълум.

Демак, биз оилада фарзанд тарбиясида ва қўни қўшнилар билан бўлган мулоқатда ассолом ўрнига интернет яхши ишламаяптими, турли ўйинлар ва норасмий оқимларга кириб кетиш ҳолатларини кўришимиз мумкин.

Шундай экан кўплам фуқароларимиз телефон орқали жабрланиб қолаётганликларини унутмаслигимиз ва хулоса қилишимиз керак. Бу борада кенг жамоатчилик ва маҳалла еттиликлари жойларда мунтазам равишда тушунтириш умумий ва виктимологик профилактик тадбирлар олиб бормоқда.

[14] Президентимиз Ўзбекистон Республикаси Конституцияси қабул қилинганлигининг 33 йиллигига бағишланган тантанали маросимдаги маърузалари

Лекин, фуқаролар ахборот олиш манбаи сифатида мурожаат қиладиган, ҳаётимизнинг ажралмас таркибий қисмига айланиб улгурган интернет хусусида баъзан кишилар бир ёқлама фикр юритаётганлиги ташвишли ҳолдир.

Айрим фуқароларимиз интернетнинг ижобий томонлари, имкониятларини ҳаддан ташқари ёқлаб, ашаддий тарафдор сифатида уни қўллаб-қувватласалар, бошқалар эса фойдаланиш жараёнида инсон оладиган негатив, салбий таъсирларга кўпроқ диққат эътибор билан ёндашмоқда.

Интернетни хавфли манба деб оладиган бўлсак, у жиноятчининг айнан манбайи сифатида намоён бўлса, ўзини англамаган ҳуқуқий таълимга эга бўлмаган Вояга етмаган шахслар ундан инсонлар ҳаётига зарарли омилларни эгалласа нима бўлади?. Ҳуқуқий билимга эга бўлган ўз-ўзлигини англаган ва интернетдан тўғри фойдаланишни билган Вояга етмаган шахслар эса одамларга хизмат қилиш мақсадида оқилона фойдаланади.

Жахон интернетнинг ривожланаётган даврда унинг функсиялари, вазифалари, имкониятларини тўғри англаш ва ундан оқилона ва тўғри мувофиқ фойдаланишни ҳар бир вояга етмаган шахслар эътиборли бўлишини хохлар эдик.

Айрим Вояга етмаган шахсларнинг интернетга тармоқларига турли ўйинларга муккасидан кетишини кун бўйи ундан мақсадсиз фойдаланиши айнан соғлиққа катта зарар эканлиги дунё янгиликларида ва Соғлиқни сақлаш томонидан берилган кўрсатувлардан хулоса қилмаётганлиги айнан ташвишли ҳолдир. Соғлиқни сақлаш тизимидан олинган маълумотга кўра Вояга етмаган шахслар кунига **6 соатдан ортиқ интернет тармоқларидан** фойдаланиши инсон учун катта хавф туғдиришини билдирган.

Жахон соғлиқни сақлаш тизимининг тавсияларига кўра, **биринчи синф ўқувчилари кунига 10 дақиқа, иккинчи-бешинчи синф ўқувчилари 15 дақиқагача компютерда ишлашлари мумкин. Ўрта умумтаълим мактабларининг 6-9-синф ўқувчилари 20–25 дақиқагача**, ўрта махсус, касб-ҳунар таълими муассасалари талабалари кунига ярим соатдан бир соатгача компютер қаршисида ўтиришлари тавсия этилади. Интернетнинг имкониятлари фақат салбий жиҳатларда акс этибгина қолмай, балки унинг ўзига хос ижобий томонлари ҳам мавжуд. Интернетнинг маълумотга дарҳол эга бўлиш, ахборот ва маълумотларнинг турфа хиллиги, шахснинг ўзини намоён қилишга ёрдам берувчи мулоқот имкониятининг мавжудлиги, таълим-тарбия борасидаги имкониятларда акс этади.

Интернетнинг ижобий томонларини инкор этмаган ҳолда, унинг энг кам сарф-харажат билан Вояга етмаган шахслар орасида самарали деструктив фаолият олиб бориш имконияти мавжудлигини ҳам таъкидлаш лозим.

Бугунги кунда Вояга етмаган шахсларимиз ҳар куни турли ижтимоий тармоқлар (“Фасебоок”, “МйСпасе”, “Twиттер”, “Ҳаббо Ҳотел”, “Фриендстер”, “Таггед.сом”, “Инстаграм”, “WҳатсАпп”, “ГАП”, “Линкедин”, “Одноклассники”, “Мой мир”, “Живой журнал”, “В контакте”, “В кругу друзей”, “Менинг оламим”, “Синфдош” ва ҳ.к.лар)да миллиардлаб инсонлар бир-бирлари билан виртуал мулоқотга киришмоқдалар, турли сайтларга кирмоқдалар,

“ЁуТубе” сингари видеохостингларга ташриф буюрмоқдалар, ҳар хил блогларда ўз фикрларини баён этиб, бошқаларнинг мулоҳазалари билан танишмоқдалар.

Вояга етмаган шахслар бузғунчи, деструктив ғояларга қарши ҳали мафкуравий иммунитет тўла шаклланмаганлигини, уларнинг эшитган ёки ўқиган маълумотига жуда тез ишонишини назарда тутсак, бу анча эътибор қаратиш долзарб масалалардан бири ҳисобланади. Ахборий-психологик хавфсизлик борасидаги бундай таҳдидларга қарши курашишда, энг аввало, ҳуқуқий асосни мустаҳкамлаш лозим, деб ҳисоблаймиз. Бу борадаги таҳдидлар доим ҳам мамлакат ичкарисидан чиқавермаслигини, уларни четдан туриб ташкиллаштиришга уриниш ҳоллари мавжудлигини ҳам ҳар биримиз доима ёдда тутушимиз зарур бўлади.

Психологлар томонидан “ахборий-қўпорувчи омил” деган тушунча истеъмолга киритилган. Ҳақиқатан ҳам интер-нетдан тарқатилаётган қўпорувчилик руҳидаги ахборотлар баъзан ҳарбий ҳаракатларни амалга оширгандан ҳам кўпроқ самара бериши мумкин.

Мазкур ахборотларнинг шахсга таъсир қилиши мумкин бўлган жиҳатлари қуйидагиларда намоён бўлади:

- кишиларнинг ахлоқий-психологик ҳола-тини, дунёқараши, сиёсий нуқтаи назари ва эътиқодини мақсадли равишда ўзгартиришга нисбатан қаратилган ахборий босим, хуруж;
- нотўлиқ, атайлаб бузилган, нотўғри маъ-лумот ва ахборотларнинг тарқатилиши;
- тўғри маълумотнинг кишилар томонидан нотўғри идрок этилишини таъминлашга интилиш.

Олимларнинг такидлашича атроф муҳит ва шахснинг ички дунёси бир-бирига чамбарчас боғлиқ бўлиб, қайсидир маънода киши хулқ-атвори характерини белгиловчи асосий омилдир. Ўзини ўзи англаш жараёнида психологик йўналтирилишга муҳтож киши учун ёнида уни танийдиган, унга оқилона маслаҳат берадиган ҳамда тўғри қарор қабул қилишда кўмаклашадиган инсон бўлиши зарурдир.

“Таълимда ва тарбияда танфус бўлмайди” акс ҳолда ёд ғоялар уни ўрнини эгаллайди. Шундай экани инсон ўзини ўзи англашда у таълим олиш, дунёқарашини кенгайтириш, турли маълумот ва материалларни қабул қилиш, янги ҳаётий тажрибани ўзлаштириш қобилиятини намоён қилади, охир-оқибатда унда инсонга хос сифатлар такомиллаштирилиб борилади.

Ахборий таъсирнинг фойда ёки зарари унинг ўзи эмас, балки кўрсатиши мумкин бўлган натижаси билан тавсифланади. Ахборий таъсир моҳияти унинг муайян жараёнларни бошқаришга нисбатан имкониятида намоён бўлади.

Вояга етмаган шахсларни интернетнинг салбий таъсиридан ҳимоялаш учун бир қатор ишларни амалга ошириш зарур. Энг аввало, талим-тарбияга ва меъёрга амал қилиш керак, яъни боланинг компютер олдида ўтказадиган вақтини белгилаб, чегаралаб бериш лозим. Шу билан бадиий, илмий китобларни ўқиш, мусиқа, спорт билан шуғулланишга ундаш мақсадга мувофиқ бўлади.

Бугунгикунда жахон интернет тармоғидаги “зомби”лар, **Алишер Навоий бобомиз таъбири билан айтганда**, “манқуртлар” пайдо бўлмаслиги учун айни

ҳолат, яъни шахсга бошқаларнинг салбий таъсир ўтказишига йўл қўймаслик мақсадида ахборот истеъмоли маданияти, мафкуравий иммунитетни таркиб топтириш ва ривожлантириш масаласи ҳануз долзарблигича қолмоқда. Мисол тариқасида интернет тармоқлари орқали содир этилаётган жиноятлар, танишув ва севги муносабатлари орқали салбий ҳолатларни келтириб чиқаришларни кўришимиз мукин. Интернет орқали содир этилаётган жиноятларнинг аксарияти 15–30 ёш оралиғидаги Вояга етмаган шахслар эканлигини кўришимиз мумкин.

Таълим муассасаларида таълим ва тарбияни қўл алоқ телефонлари ва интернетдан тўғри фойдаланиш ҳақида Профилактика инспектрлари ва Мимллий гвардия ходимлари амкорлигида бот-бот гапирилмоқда лекин, аксарият ота-оналар буни аксини қилмоқдалар.

Жумладан фарзандларига таълиб бериш, фарзандаг китоб олиб бериш ўрнига замонавий АЙФОН ПРО МАКС ва бошқа охирги моделли 15-20 млн. Сўмлик телефонлар олиб бермоқда. Бу эса фарзандларимиз оги ва тарбиясига салбий тасир кўрсатишини билмайди деб ўйлайсизми. Албата билишади, лекин келажак авлодни тарбияси биринчи ўринда туришини билмайдиган кўринади.

Хулоса ҳар-бир ота, ўз фарзандини тарбиялашда ўзини ёшлигини эслашини ва қандай қийинчиликлар эвазига шу уй-жойларни ва мартабаю мансабга эришганлигини ҳис этган ҳолда фарзандларига тўғри тарбия беришликни тавсия этаман ва мазкур ҳолатлар ўсмирлик даврида алоҳида эътибор талаб қилиш зарур. Фарзанда ота-онасини беқиёс деб билиш билан бирга кучли деб ҳисоблайди демак биз ота оналар фарзандлар ўсиш даврида инсон бирон-бир яқин кишисининг маслаҳати, маънавий қўллаб-қувватлашига эҳтиёж сезади. Албата бунда тўғри йўл кўрсатадиган инсон бўлиш шарт.

Адабиётлар:

1. Мирзиёев Ш.М. Эркин ва фаровон, демократик Ўзбекистон давлатини биргаликда барпо этамиз. Т.: “Ўзбекистон”, 2017.
2. Мирзиёев Ш.М. Буюк келажагимизни мард ва олижаноб халқимиз билан бирга қурамиз. Т.: “Ўзбекистон”, 2017.
3. Самаров Р.С. Ахборотнинг психологик хавфсизлигини таъминлаш механизми. Тошкент 2017.
4. Муминов А. Ўзбекистон ахборотлашган жамият сари. Тошкент. “Турон замин зиё” 2017.
3. Ф.Мўминов, Ш.Баротов ва бошқ. Очиқ ахборот тизимларида ахборот-психологик хавфсизлик. Дарслик. – Т.: ЖИДУ, 2013. – 196 б.
4. Шермухамедов С., Очилдиев А. Маданият ва сивилизация.- 2000.-Б.37

RAQAMLI TRANSFORMATSIYA JARAYONLARIDA KIBERXAVFSIZLIK MUAMMOLARI VA ULARNING YECHIMLARI

Tashmanov Yerlan Baymatovich

O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish institute Axborot texnologiyalar sikl katta o‘qituvchisi (PhD

Annotatsiya. Ushbu maqola raqamli transformatsiya jarayonlarida yuzaga kelayotgan kiberxavfsizlik muammolarini o‘rganish va ularni hal qilishning samarali yondashuvlarini ko‘rib chiqishga bag‘ishlangan. Asosiy e’tibor shaxsiy ma’lumotlarning xavfsizligi, tarmoq hujumlariga qarshi choralar, zararli dasturlarni aniqlash va innovatsion texnologiyalardan foydalanishga qaratilgan. Tadqiqotda sun’iy intellekt, blokcheyn va bulutli texnologiyalarning kiberxavfsizlikni ta’minlashdagi roli batafsil yoritilgan. Bundan tashqari, huquqiy va tashkiliy chora-tadbirlar ham tahlil qilinib, O‘zbekiston Respublikasining raqamlashtirish bo‘yicha tashabbuslari o‘rganilgan.

Kalit so‘zlar: raqamli transformatsiya, kiberxavfsizlik, zararli dasturlar, sun’iy intellekt, bulutli xavfsizlik, blokcheyn, O‘zbekiston qonunchiligi.

Zamonaviy jamiyatda raqamli transformatsiya jarayonlari biznes, davlat boshqaruvi va kundalik hayotning ajralmas qismiga aylandi. Ushbu jarayon yangi texnologiyalarning keng joriy qilinishi bilan birga, kiberxavfsizlikka oid muammolarni ham keltirib chiqaradi. Ma’lumotlarning ko‘payishi, ulkan tarmoqlarning kengayishi va shaxsiy ma’lumotlarning raqamli muhitda qayta ishlanishi kiberjinoyatchilikka qarshi samarali chora-tadbirlarni ishlab chiqishni talab qiladi. Raqamli transformatsiya va kiberxavfsizlikning o‘zaro bog‘liqligi iqtisodiyot, sog‘liqni saqlash, ta’lim va moliyaviy tizimlarni ham qamrab olib, muhim ahamiyat kasb etmoqda. Zamonaviy texnolgiyalar asrida deyarli barcha jinoyatlarning axborot texnologiyalari yoki internet tarmog‘idan foydalanib sodir etilishi axborot xavfsizligini ta’minlash, kiberjinoyatlarga qarshi kurashish, xalqaro hamkorlikning samaradorligini oshirishni taqozo qilmoqda. Kiberjinoyatlarning transmilliy hususiyatini inobatga olib, jahonda bu borada olib borilayotgan ilmiy tadqiqot izlanishlar axborotni xavfsiz uzatish, elektron dalillarning maqbulligi, kompyuter jinoyatlaring jinoiy-xuquqiy tavsifi, o‘zaro huquqiy yordam masalalariga bag‘ishlangan.

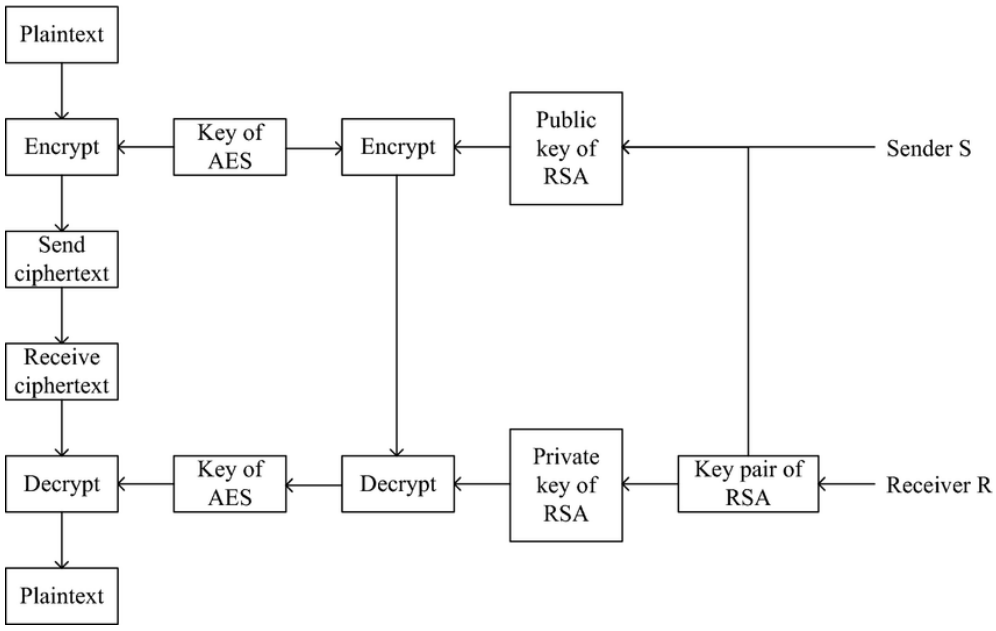
Qayd etish joizki, insonparvar huquqiy demokratik davlat va fuqarolik jamiyatini shakllantirishda axborot hamda u bilan bog‘liq bo‘lgan axborotlashtirish jarayonining huquqiy tartibga solinishi alohida ahamiyat kasb etadi. Jumladan, 2017 yil 7 fevralda qabul qilingan O‘zbekiston Respublikasi Prezidentining “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha harakatlar strategiyasi to‘g‘risida”gi Farmonida axborot xavfsizligini ta’minlash va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o‘z vaqtida va munosib qarshilik ko‘rsatish Xavfsizlik, millatlararo totuvlik va diniy bag‘rikenglikni ta’minlash hamda chuqur o‘ylangan, o‘zaro manfaatli va amaliy tashqi siyosat sohasidagi ustuvor yo‘nalishining muhim vazifasi sifatida belgilangan[3]. Shu sababli tobora avj olib

borayotgan axborot texnologiyalari sohasidagi jinoyatlarni oldini olish va ularga qarshi samarali tashkiliy-huquqiy bazani shakllantirish, axborotni xavfsiz tarqalishi uchun aniq arxitekturani yaratish dolzarb vazifalardan hisoblanadi.

Raqamli transformatsiya va xavfsizlikning yangi muammolardan ma’lumotlarning xavfsizligida raqamli tizimlarda katta hajmdagi ma’lumotlar yig‘iladi, tahlil qilinadi va saqlanadi. Shaxsiy ma’lumotlarni noqonuniy ravishda o‘g‘irlash yoki buzish kiberjinoyatchilikning asosiy yo‘nalishlaridan biri hisoblanadi. Ma’lumotlar xavfsizligini ta’minlash uchun shifrlash algoritmlarini takomillashtirish va bulutli xizmatlar xavfsizligini oshirish muhimdir. Xalqaro miqyosda 2021-yilning o‘zida ma’lumotlarning noqonuniy tarqalishi natijasida korxonalar 4 milliard dollar zarar ko‘rgan ma’lumotlarni shifrlash va ma’lumotlar bazalariga ruxsat etilgan kirishni ta’minlash ushbu muammolarni kamaytirishga yordam beradi.

Tarmoq hujumlari va kiberjinoyatlarni raqamli transformatsiya bilan bog‘liq tarmoqlar sonining oshishi bilan DDoS hujumlar va fishing hujumlari keng tarqalgan. Ushbu hujumlar tizimlarning ishlashini sekinlashtiradi va ulardan ma’lumotlar o‘g‘irlanadi. DDoS, fishing va botnetlar kiberxavfsizlikning asosiy muammolari hisoblanadi. Misol uchun, 2023-yilda global miqyosda 15 milliondan ortiq DDoS hujum qayd etilgan . Tarmoqya qilish uchun IDS (Intrusion Detection Systems) va IPS (Intrusion Prevention Systems) tizimlari keng qo‘llaniladi.

Zararli dasturlar (malware) yangi dasturiy ta’minot va ilovalarni joriy etish bilan zararli dasturlarni tizimlarga kirib olish ehtimoli oshadi. Ayniqsa, shifrlovchi dasturlar (ransomware) o‘zining xavf darajasini oshirmoqda. Shifrlovchi dasturlar (ransomware) ayniqsa katta xavf tug‘diradi. Ushbu dasturlar foydalanuvchi ma’lumotlarini shifrlab, to‘lov talab qiladi. Masalan, 2022-yilda kiberjinoyatchilik sabab 71 foiz tashkilot shifrlovchi dasturlardan zarar ko‘rgan.



1 Rasm AES + RSA algoritmining shifrlash va shifrni ochish oqimi

Kiberxavfsizlik muammolarini hal qilish yondashuvlardan biri bu texnologik yondashuvlarda shifrlash va autentifikatsiya: Shaxsiy va tijorat ma’lumotlarini xavfsiz saqlash uchun shifrlash algoritmlaridan foydalanish. Masalan, Advanced Encryption

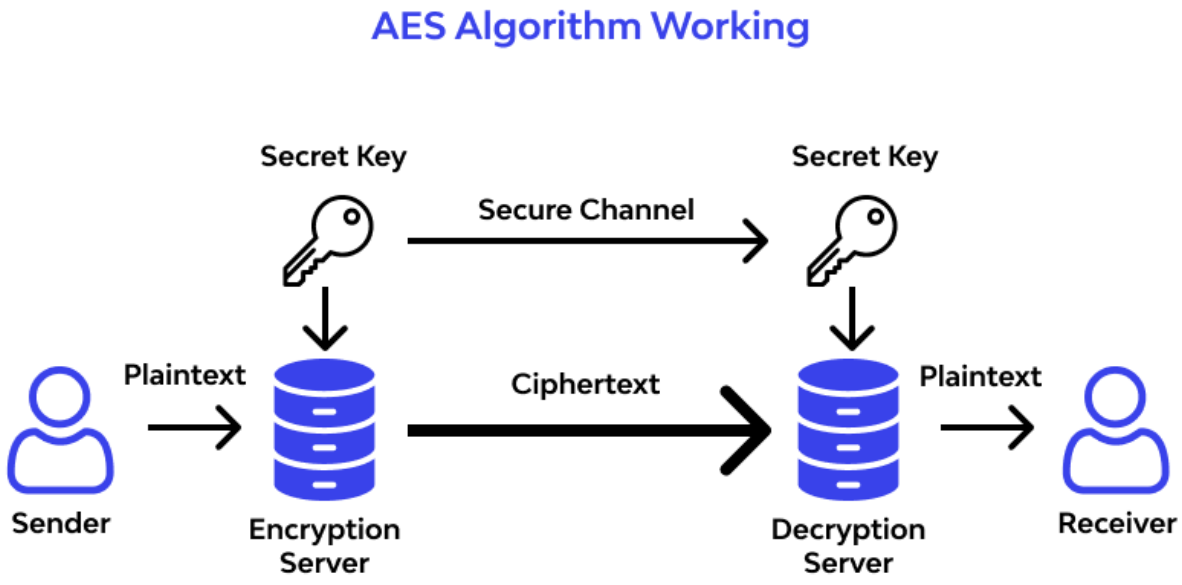
Standard (AES) va Rivest-Shamir-Adleman (RSA) algoritmlari ma’lumotlarning xavfsizligini ta’minlash uchun ishlatiladi. Bulutli texnologiyalarda shifrlash alohida ahamiyatga ega. IDS/IPS tizimlari esa tarmoq hujumlarini aniqlash va bloklashda samarali vosita sifatida ishlatiladi. Yani IDS tarmoqqa bo‘ladigan har qanday hujumni aniqlaydi, IPS esa ushbu hujumlarni real vaqt rejimida bloklaydi.

AES 128 shifrlashda 128-bitli AES sirini 128-raqamli AES shifrlash bilan oddiy matnli faktlarni kodlashning eng ko‘zga ko‘ringan usuli.

Umumiy qoida sifatida, 128 raqamli AES shifrlash, shuningdek, AES shifrlash indeksining yaxshi to'rtburchaklar uzunligi ekanligini ta'kidlashi mumkin. AES bilan aralashtirilgan ma'lumotlarning to'rtburchaklar uzunligi hali ham 128 qismdan iborat bo'lib, AES kalit uzunligi uchun kam to'laydi - 128, 192 va 256 uyalar - ta'sir qiladi.

987 AES 128-tsikl shifrlash - bu AES shifrlashning uchta shaklining maksimal beqarorligi: 128-bit, 192-bit va 256-raqamli. Shifrlash AES , shu tarzda har bir kichik yaxshilanish taqdim etilgan xavfsizlik uchun shifrlash uchun qo'shimcha sozlamalardan foydalanadi. 128 tsiklli AES shifrlash har doim ham barqaror bo'lmasligi yoki ma'lumotlaringizni shifrlashning ajoyib istagi har doim ham shart emas; 128 raqamli AES kalitining narxini olish uchun milliardlab yillar ketishi mumkinligini yodda tuting. U yo'naltiruvchi hokimiyat ma'lumotlarini kodlash uchun keng qo'llaniladi, shuning uchun uning chidamliligiga ishonch hosil qilishingiz mumkin.

AES 192 shifrlashda 192 qismli AES kaliti bilan ochiq matnli yozuvlarni kodlash yondashuvi 192 qismli AES shifrlash deb nomlanadi. Milliy Xavfsizlik Agentligi (NSA) 192 qismli AES shifrlashdan foydalanadi, bu esa ochiq matnni shifrlangan matnga chiqarish uchun yana 12 turni maqsad qilib qo'yadi va bog'liqlik to'qimasini saqlash, yashirish va ajoyib tarzda qoplanishini ta'minlaydi.



2-Rasm. AES shifrlash turlari va ularning ishlash usulli.

128-bit, 192-bo‘lak va 256-raqamli AES shifrlash o‘rtasida 192-bo‘lakli AES shifrlash odatda barqaror bo‘lgan ikkinchi o‘rinda turadi va u 256-sikli AES shifrlashiga yaqin bo‘lib, hayratlanarli darajada cheklangan statistik ma’lumotlarni shifrlash uchun zarur bo‘lgan asosiy muddat hisoblanadi.

Agar 128 tsiklli AES shifrlash kuchli bo'lsa va superkompyuterning uzilishi uchun milliardlab yillar kerak bo'lsa, siz 192 qismli AES shifrlash yoki 256 raqamli AES shifrlash uchun asosli sababni so'rashingiz mumkin.

Ta'sirchan yozuvlarni olishga kelsak, ko'pchilik mijozlar 128 tsiklli AES shifrlash ularning savollariga javob berishini aytadilar. Vayronagarchilik ehtimoli eng past darajadami yoki yo'qmi. Xuddi shu vaqtda, kamdan-kam sezgir yozuvlar shaklni kiritadi; hatto keng va katta yig'ilgan yozuvlarning yaxshi ma'lum bo'lgan kelishuvi ham hukumatning muhim yurish shartlarini qabul qilishga ikkilanadigan xavfdir. Shunga ko'ra, ular uzoqroq AES kalit uzunliklaridan foydalanadilar, bu esa qo'shimcha muhim xavfsizlik va bo'sh joy qidirishda qo'shimcha muhim monster elektr energiyasini ta'minlaydi. Bu, ehtimol, kvantni tasdiqlash hujumlariga e'tibor qaratadigan tashkilotni etkazish uchun mashhurlikka ega bo'lgan boshdir.

AES 256 shifrlash bu AES baholash va 256 AES kalit uzunligi yordamida ochiq matn faktlarini yashirish usuli odatda 256 tsiklli AES shifrlash sifatida tavsiya etiladi. nazariy jihatdan xavfli. Qolaversa, bu eng boshqarish mumkin bo'lgan, eng qiyini. Oddiy matnni shifrlangan matnga chiqarish uchun 256 tsiklli AES shifrlash 14 ta muhim sozlamalardan foydalanadi. Milliy xavfsizlik agentligi (NSA) ulardan har qanday triller va muqobil ravishda haqiqiy hukumat ichidagi ma'lumotni kafolatlash uchun foydalanadi, lekin unutmangki, aslida muhim bo'lgan narsa har tomonlama hujum qilish qiyin.

Kalitning uzunligi tufayli 256-tsiklli AES shifrlash 3 ta variantdan eng elektr ta’minlangani hisoblanadi: 128-bitli, 192-qismli, 256-raqamli AES shifrlash. Ba’zilar, umuman olganda, bu ahmoqlik nima ekanligini tasavvur qilishadi. AES 256 tsiklli shifrlashni dahshatli jismoniy hujum bilan sindirish uchun milliardlab yillar kerak bo'lishini kafolatlaydigan foydasiz ko'plik deb atash mumkin.

Ammo boshqariladigan, tasniflanmagan va muvofiqlashtirilgan mato kodlash, ajoyib davlat hukumati, bizning tanamiz va rasm millati bilan bir vaqtda, bazaviy modelerlar 256 raqamli AES shifrlashni tanlaydilar, lekin unutmangki, bu eng zo'r shifrlash. sindiradi va uchta AES kalit uzunligi o'lchamining ajoyib xavfsizligiga ega.

Foydalanuvchilarni o‘qitish va xabardorlik darajasi Social engineering hujumlariga qarshi kurash uchun foydalanuvchilarning kiberxavfsizlik bo‘yicha bilimlarini oshirish. Bunda Social engineering hujumlariga qarshi treninglar tashkil etish, foydalanuvchilarni zararli dasturlarni aniqlashga o‘rgatish kiberjinoyatchilikning kamayishiga hissa qo‘shadi. Misol uchun, "Google Cybersecurity Action Plan" foydalanuvchilarni xabardor qilishni kuchaytirishga qaratilgan. Foydalanuvchilarga zararli havolalarni aniqlash va ulardan saqlanish bo‘yicha ko‘rsatmalar berish.

Innovatsion texnologiyalarni joriy etish sun’iy intellekt kiberxavfsizlik tizimlarida hujumlarni prognoz qilish va real vaqt rejimida oldini olish uchun ishlatiladi. Hozir kunda sun’iy intellekt tarmoq hujumlarini prognozlash va zararli dasturlarni aniqlashda katta imkoniyatlarni taqdim etadi. Mashina o‘rganish asosida

ishlab chiqilgan algoritmlar kiberjinoyatlarning 95 foizgacha aniqlanishini ta’minlashi mumkin .

Bulutli xavfsizlik jihatidan SaaS xizmatlari va bulutli texnologiyalar yordamida ma’lumotlarning xavfsizligini ta’minlash. Bulutli xizmatlardan foydalangan holda real vaqt rejimida tizimlarni himoya qilish imkoniyati yaratiladi. Bu esa korxonalar uchun katta iqtisodiy samaradorlikni ta’minlaydi.

Blokcheyn texnologiyasi ma’lumotlar bazalarining himoyasini kuchaytirish va tizimning buzilmasligini ta’minlash uchun ishlatiladi. Blokcheyn texnologiyasi ma’lumotlar bazalarining buzilmasligini ta’minlaydi. U tranzaksiyalarni real vaqt rejimida kuzatish va qayta ishlash imkoniyatini beradi, bu esa tizimlarning barqarorligini oshiradi.

Raqamli transformatsiya jarayonlari global taraqqiyotga katta hissa qo‘shadi, lekin ular bilan birga kiberxavfsizlik xavflari ham ortib bormoqda. Ushbu muammolarni hal qilish uchun texnologik, huquqiy va tashkiliy choralarni uyg‘unlashtirish zarur. Innovatsion yondashuvlar va xalqaro hamkorlik raqamli xavfsizlikni ta’minlashda muhim rol o‘ynaydi. Shunday qilib, raqamli transformatsiyaning samaradorligini oshirish va uning barqaror rivojlanishini ta’minlash uchun har tomonlama kompleks strategiyalar ishlab chiqilishi zarur.

Foydanilgan adabiyotlar

1. S.Morgan. Official Annual Cybercrime Report 2019 // Cybersecurity Ventures.
2. https://www.statista.com/ (The Statistics Portal).
3. O‘zbekiston Respublikasi Prezidentining 2017 yil 7 fevraldagi PF-4947-son “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida”gi Farmoni. O‘zbekiston Respublikasi qonun hujjatlari to‘plami, 2017 y., 6-son, 70-modda.
4. Symantec Internet Security Threat Report, 2021.
5. Cisco Annual Cybersecurity Report, 2023.
6. McAfee Threat Report, 2022.
7. Google Cybersecurity Study, 2022.
8. Palo Alto Networks Research, 2023.

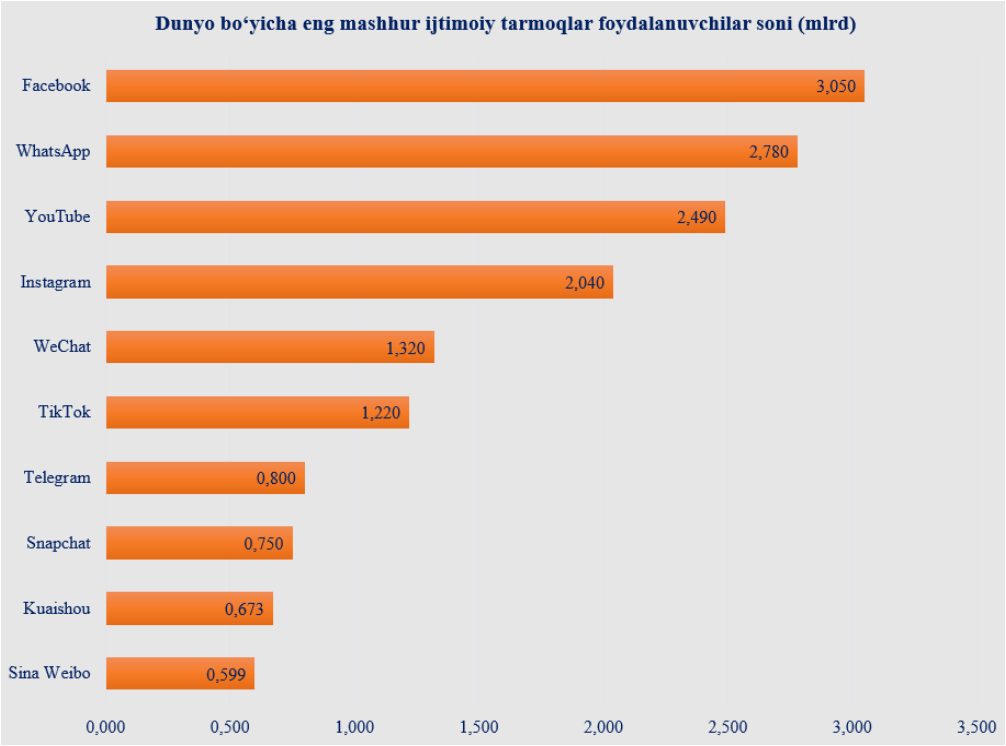
FACEBOOK IJTIMOIY TARMOG‘IDAN MA’LUMOTLARNI IZLASH VOSITALARI

Risqaliyev Jaxongir Dadajon-o‘g‘li

Ichki ishlar vazirligi Malaka oshirish instituti katta o‘qituvchisi

2024-yilga kelib dunyo bo‘yicha umumiy ijtimoiy tarmoqlardan foydalanuvchilar soni 5,17 milliard kishiga yetdi [3]. Bu esa ijtimoiy tarmoqlarning ta’siri va imkoniyatlari kengligini anglatadi. Ijtimoiy tarmoqlardagi ma’lumotlardan to‘g‘ri va samarali foydalanilsa, insonlar yoki tashkilotlar uchun qimmatli axborotlarni taqdim etadi. Bugungi kunda Facebook ijtimoiy tarmog‘i 3 milliarddan oshiq foydalanuvchi hisobiga, mashhurligi bo‘yicha dunyoda birinchi o‘rinda turibdi (1-rasm) [4]. Bu ijtimoiy tarmoqqa 2004-yilda Mark Sukerberg, Eduardo Saverin, Dastin

Moskovits va Kris Xyuzlar tomonidan asos solingan. Ijtimoiy tarmoq butun dunyoda ommalashgani bois, Mark Sukerbergni 23 yoshida dunyoning eng yosh milliarderiga aylantirdi.



1-rasm. Dunyo bo‘ylab eng mashhur ijtimoiy tarmoqlar ro‘yxati

Facebook ijtimoiy tarmog‘ini tushunish va ishlatish juda osondir. Facebook foydalanuvchi akkauntida ko‘plab ma’lumotlarni topish mumkin. Masalan, Facebook akkauntini yaratish uchun elektron pochta (yoki telefon raqam), foydalanuvchi nomi, parol, tug‘ilgan kun va jinsini kiritishi kerak. Facebook akkauntini faollashtirgandan so‘ng ish va ta’lim ma’lumotlari, yashash joyi, aloqa ma’lumotlari (elektron pochta, telefon raqami, manzil, shifrlangan xabarlarni qabul qilish uchun ochiq kalit), diniy va siyosiy ma’lumotlar kabi qo‘shimcha ma’lumotlarni qo‘shish mumkin [2].

Facebookning 2020-yilda qayta ishlangan dizayni onlayn tadqiqotchilar uchun foyda keltirishi mumkin bo‘lgan ko‘plab yangi qidiruv imkoniyatlarini taqdim etdi [1]. OSINT (Open source intelligence) dasturiy vositalari yordamida Facebook ijtimoiy tarmog‘idan ma’lumotlarini olish, tahlil qilish va vizualizatsiya qilish mumkin.

Facebook ijtimoiy tarmog‘idan ma’lumotlarni izlash uchun avvalo ro‘yxatdan o‘tish kerak. Ro‘yxatdan o‘tishda soxta ma’lumotlardan foydalanish lozim, chunki shaxsiy profildagi ma’lumotlar oshkor bo‘lishi va akkaunt bloklanib qolishi mumkin. Buning uchun quyidagi ishlarni bajarish kerak:

1. Dastlab https://fakeit.receivefreesms.co.uk/c/us/_kabi soxta ma’lumotlar tayyorlab beruvchi veb-saytga o‘tish va kerakli davlatni tanlash lozim.

2. Facebook.com saytiga kirish va ro‘yxatdan o‘tish tugmasini bosiladi.

3. 1-bosqichda veb-saytni ochishda olgan soxta ma’lumotlardan, shu jumladan elektron pochtani kiritish kerak. Soxta pochta uchun facebook.com saytidan kod jo‘natiladi va shu kod kiritiladi. Shuningdek, tasdiqlashni telefon raqam orqali ham amalga oshirish kerak. Onlayn virtual telefon raqamlarni

https://onlinesim.io/ saytidan olish mumkin. Shunday qilib, Facebook ijtimoiy tarmog‘ida OSINT uchun paypoq qo‘g‘irchog‘i (Sock Puppets) yaratiladi.

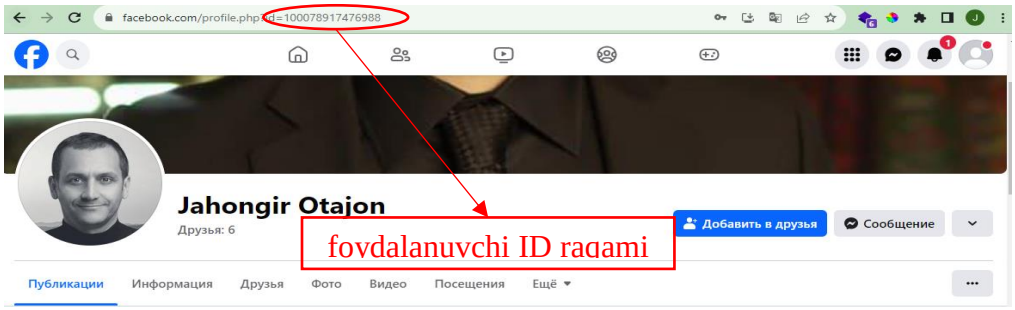
4. https://thispersondoesnotexist.com/ saytiga o‘tib, soxta akkauntning profiliga ishlatiladigan rasmlar olinadi.

5. Facebook akkauntidagi profilga yana bir qancha soxta ma’lumotlar qo‘shilsa, profil haqiqiy va shubhali ko‘rinmaydi [5].

Facebook ijtimoiy tarmog‘idan ma’lumot izlashni har doim kompyuterdan amalga oshirish lozim. Ba’zida ayrim odamlar o‘zlarining elektron pochta manzillari va telefon raqamlarini hammaga ochiq qilib qo‘yishadi, shuning uchun dastlab nishondagi profilning aloqa va asosiy ma’lumotlar bo‘limini ko‘zdan kechirish zarur. Facebook ijtimoiy tarmog‘i uchun eng yaxshi OSINT dasturiy vositalari quyidagilardir:

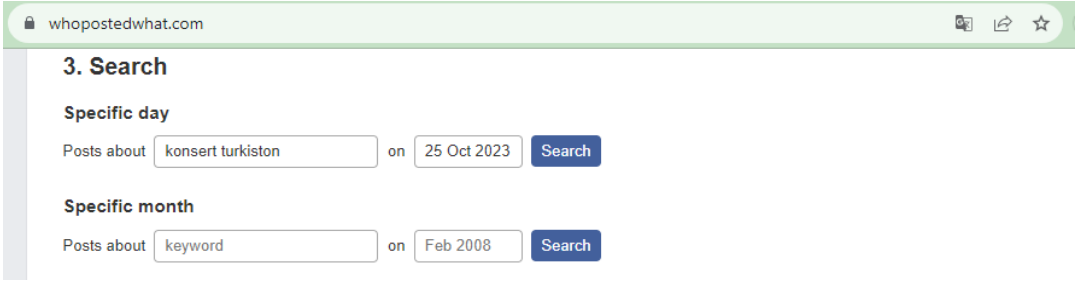
- Lookup-id.com
- Whopostedwhat.com
- Intelligence X
- Exportcomments.com

Lookup-id.com. Facebookda foydalanuvchi ID raqamini topish juda oddiy. Buning uchun o‘sha foydalanuvchining profiliga kiriladi va URL manzili orqali aniqlanadi (2-rasm). Lookup-id.com sayti Facebook foydalanuvchisi yoki kanallarning noyob ID raqamini topadi [6]. ID raqami ko‘rsatilmagan kanal yoki profillarni URL manzilidan nusxa olib, https://lookup-id.com/ saytiga qo‘yiladi va sayt ID raqamni aniqlab beradi.



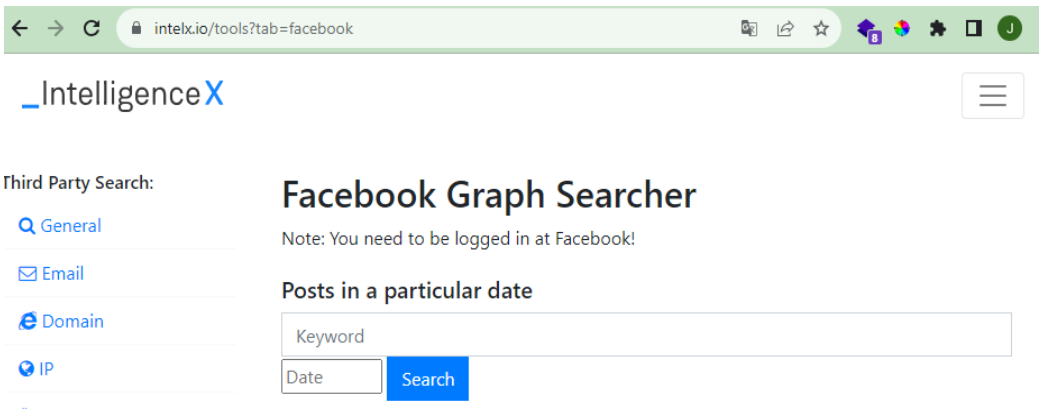
2-rasm. Facebook foydalanuvchisi profili

Whopostedwhat.com. Tanlangan vaqt oralig‘ida kalit so‘zlar bo‘yicha postlarni qidirishga ruxsat beradi [7]. Ushbu tadqiqot vositasi Facebook ijtimoiy tarmog‘idan kalit so‘zlarni qidirishga yordam beradi. Tadqiqotchi veb-saytga kirgandan so‘ng, ma’lum sanalarga mos keladigan kalit so‘zlarni qidirishi mumkin (3-rasm).



3-rasm. Whopostedwhat.com sayti interfeysi

Intelligence X. Intelx.io sayti har qanday tadqiqotchi ishlatishi mumkin bo‘lgan ochiq kodli dasturiy vositadir [8]. Unda kalit so‘zlarni kun, oy, yil oralig‘i bo‘yicha yoki ID raqamni kiritish orqali qidirish mumkin (4-rasm).



4-rasm. Intelligence X sayti interfeysi

Exportcomments.com. Exportcomments.com sayti Facebook ijtimoiy tarmog‘ida qoldirilgan sharhlarni CSV fayliga eksport qilib beruvchi pullik onlayn saytdir (5-rasm) [9]. 100 tadan kam bo‘lgan sharhlarni bepul amalga oshiradi.

5-rasm. Exportcomments.com sayti interfeysi

Xulosa. Facebook eng mashhur ijtimoiy tarmoq bo‘lganligi sababli ko‘proq ma’lumot izlayotganlar uchun foydali manbadir. So‘nggi vaqtlarda mutaxassislar tomonidan “DumpltBlue+” va “IG Follower Export Tool” kabi brauzer kengaytmalari taqdim etildi [10]. Bu qo‘shimcha vositalar yordamida tadqiqotchilar Facebook ijtimoiy tarmog‘idan foydali ma’lumotlarni olishlari mumkin. Ta’kidlash joizki, Meta kompaniyasi doimiy ravishda Facebookdan foydalanishni yanada xavfsizroq qilish va foydalanuvchi ma’lumotlarini himoya qilish ustida ishlamoqda, ammo baribir hech kim kuzatuv yoki tahlildan himoyalanmagan.

Foydalanilgan adabiyotlar ro‘yxati:

1. M.Bazzell. Open source intelligence techniques. Eighth edition.
2. N.A.Hassan, R.Hijazi. Open source intelligence methods and tools. A practical guide to online intelligence. 2018. https://doi.org/10.1007/978-1-4842-3213-2
3. https://www.forbes.com/advisor/business/social-media-statistics/
4. https://buffer.com/library/social-media-sites/
5. https://hacklido.com/blog/313-facebook-osint-use-facebook-like-a-pro

6. https://www.osintessentials.com/facebook
7. https://www.liferaftinc.com/blog/9-best-osint-software-tools-for-facebook
8. https://securitytrails.com/blog/osint-facebook-tools
9. https://telegra.ph/facebook-meta-osint-thread--010-12-07?source=post_page-----2da36d20890c----------
10. https://os2int.com/toolbox/identifying-and-extracting-data-with-the-facebook-and-instagram-osint-add-on/

KRIPTOJEKING HUJUMLARINING TAHLILI

Risqaliyev Jaxongir Dadajon-o‘g‘li

Ichki ishlar vazirligi Malaka oshirish instituti katta o‘qituvchisi

Annotatsiya. Maqola kriptojeking hujumlariga bag‘ishlangan bo‘lib, uning mohiyati, sodir etish usullari va aniqlash hamda oldini olish yo‘llari haqida so‘z yuritadi. Kriptojeking – bu kiberjinoyatchilar tomonidan foydalanuvchining qurilmalarida yashirin tarzda kripto-aktivlarni mayning qilish jarayonidir. Maqolada shuningdek, kriptojekingni amalga oshirishda ishlatiladigan zararli dasturiy ta'minotlar va ulardan himoyalanish usullari yoritilgan.

Kalit so‘zlar: kripto-aktiv, kriptojeking, kiberjinoyat.

Kirish. So‘nggi yillarda kripto-aktivlarning ommalashishi bilan birga, bu turdagi jinoyatlar ham ko‘payib bormoqda. Bu holat kiberxavfsizlikka oid yangi usullarni ishlab chiqishni va bu sohada ilmiy izlanishlarni kengaytirishni talab etmoqda. Kripto-aktivlar markazlashtirilmaganligi sababli ularni o‘zlashtirish jarayonida rasmiy nazoratning yo‘qligi jinoyatchilarga qo‘l kelmoqda. Shu sababli, davlatlar va xalqaro tashkilotlar jinoyatchilikka qarshi kurashish uchun yangi qonuniy va texnik mexanizmlarni ishlab chiqishga intilmoqda. Kripto-aktiv yordamida vositachilarga ehtiyoj sezmasdan xavfsiz onlayn tranzaksiyalarni amalga oshirishni osonlashtiradi. “Kripto” atamasi bu yozuvlarni himoya qiladigan hamda uchinchi tomon vositachilarni boshqaradigan turli xil shifrlash algoritmlari va kriptografik usullarni anglatadi.

O‘zbekiston Respublikasida Istiqbolli loyihalar milliy agentligi kripto-aktivlar aylanmasi sohasini rivojlantirish hamda ushbu sohada faoliyatni litsenziyalash va ruxsat berish tartib-taomillari bo‘yicha vakolatli organ hisoblanadi. O‘zbekistonda “kriptovalyuta” atamasi o‘rniga “kripto-aktiv” atamasi qo‘llanilgan va unga agentlik tomonidan quyidagicha ta’rif berilgan:

Kripto-aktiv - ma’lumotlarning taqsimlangan reyestridagi raqamli yozuvlar yig‘indisi bo‘lgan, qiymati va egasiga ega mulkiy huquq [1].

Kripto-aktivlarga 2 xil usulda ega bo‘lish mumkin:

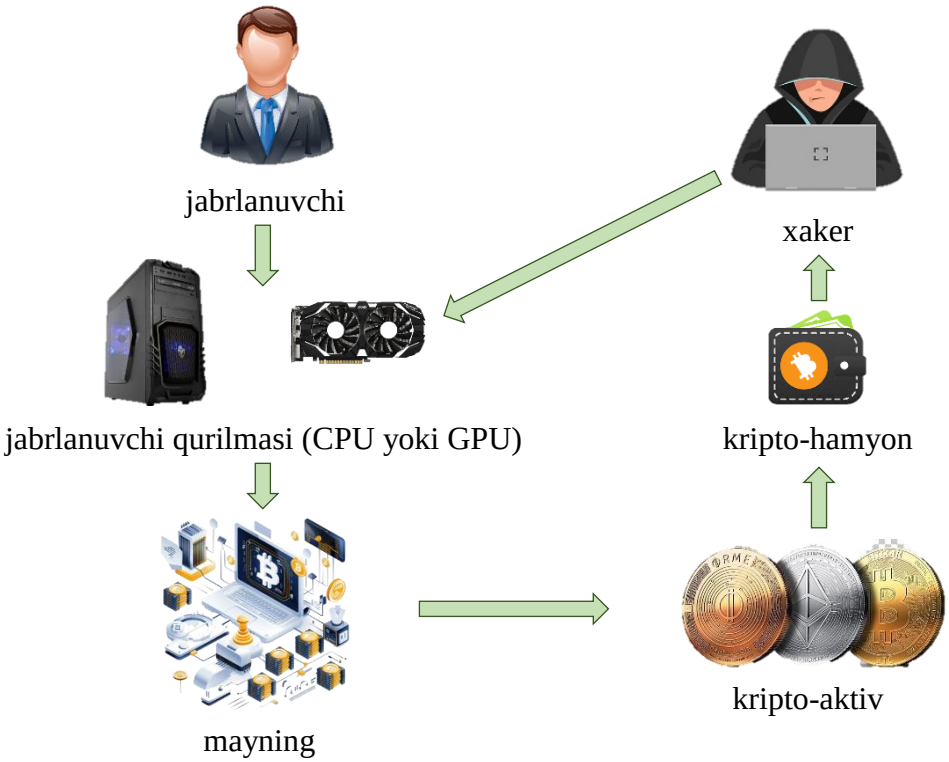
1) mayning;

2) kripto-aktiv ayirboshlash birjalaridan sotib olish.

Mayning - hisoblash operatsiyalarini bajarish orqali ma’lumotlarning taqsimlangan reyestrini yuritish, bloklarning yaxlitligini yaratish va tasdiqlash faoliyati [2].

Mayning jarayonida ishtirokchilar masalaning murakkabligini yechish uchun o‘z qurilmalarini va katta miqdordagi elektr energiyasini sarflashlari kerak bo‘ladi. Ushbu masalani birinchi bo‘lib yechganlar kripto-aktivga ega bo‘ladi [3, 36-b].

Kripto-aktivlar orqali foyda olish maqsadida o‘ziga jinoyatchilarni ham jalb qilmoqda. Ular foydalanuvchilarning kompyuterlaridan, smartfonlaridan yoki boshqa qurilmalaridan sezdirmasdan zararli dasturiy ta’minot (mayner dasturi)ni ishga tushirib, mavjud resurslardan foydalangan holda daromad olishlari mumkin (1-rasm). Bu strategiya kriptojeking deb nomlanadi [4].



1-rasm. Kriptojeking hujumi sxemasi

Kriptojekingni amalga oshirish uchun kiberjinoyatchilar bir qancha usullardan foydalanishlari mumkin. Eng keng tarqalgan usullar:

- **Brauzerga asoslangan kriptojeking:** Zararli skriptlar veb-saytlarga joylashtiriladi va foydalanuvchi veb-saytga tashrif buyurganida avtomatik ravishda ishga tushadi. Brauzer resurslaridan foydalanib, murakkab matematik muammolarni yechish orqali kripto-aktiv olinadi [5, 6].
- **Dasturga asoslangan kriptojeking:** Zararli dastur foydalanuvchi qurilmasiga o‘rnatiladi va mayning uchun foydalaniladi. Bu odatda fishing kabi ijtimoiy muhandislik usullari orqali amalga oshiriladi [6, 7].
- **Gibrid usul:** Xakerlar yuqoridagi usullarning kombinatsiyasidan foydalanishlari mumkin [8]. Masalan, yuzlab qurilmalar hujumchi uchun kripto-aktiv mayninggi bilan shug‘ullanayotgan bo‘lsa, ularning 10% maqsadli qurilmalarda o‘rnatilgan kod orqali, 90% esa veb-brauzerlari orqali daromad keltirishi mumkin.

Kriptojekingni aniqlash uchun turli xil usullar mavjud. Ba’zilari quyidagilar:

- **CPU (Central processing unit) foydalanishini kuzatish:** Kriptojeking qurilmaning protsessor quvvatidan foydalanishi sababli, CPU foydalanishining g‘ayritabiiy darajada yuqori bo‘lishi kriptojekingning belgisi bo‘lishi mumkin.
- **Tarmoq trafigini tahlil qilish:** Kriptojeking dasturlari odatda mayningda internetga bog‘lanadi. Ushbu trafikni tahlil qilish kriptojekingni aniqlashga yordam berishi mumkin.
- **Xavfsizlik dasturlaridan foydalanish:** Antivirus dasturlari va boshqa xavfsizlik dasturlari kriptojeking dasturlarini aniqlash va bloklashga yordam berishi mumkin.

Xulosa. Kriptojeking kiberjinoyatchilar uchun daromadli kiberjinoyat bo‘lib, tobora ommalashib bormoqda. Foydalanuvchilar kriptojekingdan himoyalanish uchun yuqorida sanab o‘tilgan choralarni ko‘rishlari kerak. Bundan tashqari, kriptojekingni aniqlash hamda oldini olish uchun yangi texnologiyalar va usullarni ishlab chiqish muhimdir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. O‘zbekiston Respublikasi Istiqbolli loyihalar milliy agentligi direktorining 2022-yil 24-noyabrdagi “*O‘zbekiston Respublikasi rezidentlari tomonidan kripto-aktivlarni chiqarish, chiqarishni ro‘yxatdan o‘tkazish va muomalaga kiritish tartibi to‘g‘risidagi nizomni tasdiqlash haqida*” 61-son buyrug‘i.
2. O‘zbekiston Respublikasi Istiqbolli loyihalar milliy agentligi direktorining 2023-yil 20-sentabrdagi “*Mayning faoliyatini amalga oshirish uchun ruxsatnoma berish tartibi to‘g‘risidagi nizomni tasdiqlash to‘g‘risida*” 68-son buyrug‘i.
3. Taniyev A. Blokcheyn texnologiyasi va kriptovalyutalar. *O‘quv qo‘llanma.* - Samarqand: SamDU nashri, 2021. – 192 bet.
4. Konoth R. K., Vineti E., Moonsamy V., Lindorfer M., Kruegel C., Bos H. and Vigna G. An in-depth look into drive-by mining and its defense. In Proc. of ACM. *Conference on Computer and Communications Security (CCS)*, Oct. 2018.
5. Caprolu M., Raponi S., Oligeri G., Pietro R.D. Cryptomining Makes Noise: a Machine Learning Approach for Cryptojacking Detection. *Computer Communications Vol. 171*. 2021. Pages 126-139.
6. Babenko T., Kolesnikova K., Lisnevskyi R., Makilenov Sh. and Landovsky Y. Definition of Cryptojacking Indicators. https://ceur-ws.org/Vol-3680/S4Paper6.pdf
7. Kadhum L.M., Firdaus A., Hisham S.I., Mushtaq W., Razak M.F. Features, Analysis Techniques, and Detection Methods of Cryptojacking Malware: A Survey. *International journal on informatics visualization.* 2024. Pages 891-896.
8. https://www.imperva.com/learn/application-security/cryptojacking/

SERVERLAR QURILMALARIDAGI KIBERJINOYATLARINI ANIQLASH USULLARI

Boynazarov Otabek Murot o‘g‘li

IIV Malaka oshirish instituti, Axborot texnologiyalari sikli o‘qituvchisi
e-mail:boynazarovotabek0712@mail.ru

Zamonaviy dunyoda axborot texnologiyalari rivoji bilan birga kiberjinoyatlar ham ortib bormoqda. Serverlar, tashkilotlarning asosiy ma’lumotlarini saqlovchi va boshqaruvchi muhim infratuzilma sifatida, kiberhujumlar uchun asosiy nishonlardan biriga aylangan. Bu jarayonda serverlarning xavfsizligi va ularni muntazam nazorat qilish dolzarb masalaga aylandi.

Kiberjinoyatlar tashkilot ma’lumotlarining o‘g‘irlanishi, zararli dasturlar orqali tizim faoliyatining buzilishi va tarmoq infrastrukturasi zaifliklaridan foydalanishni o‘z ichiga oladi. Shu sababli, serverlarda yuzaga kelishi mumkin bo‘lgan tahdidlarni aniqlash, ularga qarshi choralar ko‘rish va zararni minimallashtirish muhimdir.

Mazkur maqolada serverlarda bo‘layotgan kiberjinoyatlarni aniqlashning asosiy usullari va zamonaviy yondashuvlar yoritib berilgan. Ushbu yo‘nalishlar nafaqat kiberjinoyatlarning oldini olishga, balki tashkilotning xavfsizlik siyosatini mustahkamlashga ham xizmat qiladi. Serverlarda bo‘layotgan kiberjinoyatni aniqlash uchun maxsus vositalar va usullar kerak bo‘ladi. Quyida kiberjinoyatlarni aniqlashning asosiy yo‘llari keltirilgan:

1. Loglarni tahlil qilish
2. Anomaliyalarni aniqlash
3. Zaifliklarni aniqlash vositalari
4. Kirishni kuzatish
5. IDS/IPS tizimlaridan foydalanish
6. Zararli dasturlarni aniqlash
7. Tarmoq va port monitoringi
8. Kriptografik faoliyatni tekshirish
9. Foydalanuvchi faoliyatini tahlil qilish
10. Huquqbuzarlikni tasdiqlovchi belgilar
11. Tahlil va xabar berish vositalari

Server xavfsizligini ta’minlash muammolari IT infratuzilmasini boshqarishda jiddiy e’tibor talab qiladi, chunki har bir zaiflik kiberhujumlar uchun imkoniyat yaratadi.

1. **Zaif parollar va kirish boshqaruvi**

- ***Zaif parollar:*** Oson taxmin qilinadigan yoki takrorlanadigan parollardan foydalanish serverga ruxsatsiz kirishni osonlashtiradi.
- ***Kirish huquqini boshqarishning etishmasligi:*** Foydalanuvchilarga kerak bo‘lmagan ruxsatlar berilishi xavfsizlikni pasaytiradi. Minimal huquq prinsipi (least privilege) qo‘llanilmagan hollarda foydalanuvchilar tomonidan noto‘g‘ri foydalanish xavfi ortadi.

2. **Yangilanishlarning o‘z vaqtida o‘tkazilmasligi**

- ***Dasturiy ta’minot zaifliklari:*** Har bir yangilanish odatda ilgari aniqlangan zaifliklarni bartaraf etadi. Yangilanishlarni qoldirish xakerlarga bu zaifliklardan foydalanish imkonini beradi.
- ***Avtomatlashtirilmagan jarayonlar:*** Yangilanishlarni qo'lda boshqarish vaqt o‘tishi bilan e'tibordan chetda qolishi yoki kechiktirilishi mumkin.

3. **Ko‘p foydalanuvchi faoliyati**

- ***Ichki xavflar:*** Tizimda ko‘p foydalanuvchilar mavjud bo‘lsa, ularning biri zararli niyatda bo‘lishi ehtimoli ortadi. Shu sababdan, foydalanuvchilarni muntazam monitoring qilish zarur.
- ***Auditsiz faoliyat:*** Foydalanuvch i faoliyatini audit qilmaslik potentsial xavfli harakatlarni aniqlashni qiyinlashtiradi.

4. **Noto‘g‘ri konfiguratsiyalar**

- ***Standart sozlamalar:*** Server sozlamalarini o‘zgartirmaslik xavfsizlik teshiklariga olib kelishi mumkin. Masalan, standart admin akkauntini saqlab qolish xavfli.
- ***Shifrlanmagan ulanishlar:*** Tarmoq orqali uzatiladigan ma’lumotlarning shifrlanmasligi ma’lumotlarning o‘g‘irlanishiga sabab bo‘ladi.

Ushbu muammolarni bartaraf etish bo‘yicha yechimlar:

✓ Kuchli parol siyosatini joriy etish va ikki faktorli autentifikatsiyani (2FA) qo‘llash.

✓ Dasturiy ta’minotni muntazam yangilash va avtomatlashtirilgan yangilanishlarni sozlash.

✓ Minimal huquq prinsipi asosida foydalanuvchi kirishini boshqarish.

✓ Konfiguratsiyalarni muntazam ravishda ko‘rib chiqish va xavfsizlik standartlariga muvofiqlashtirish.

✓ Foydalanuvchi faoliyatini doimiy kuzatish va audit jarayonlarini avtomatlashtirish.

Server xavfsizligi doimiy monitoring va yangilanishlarni talab qiladi. Muammolarni o‘z vaqtida aniqlash va yechim choralarini ko‘rish tizimni himoya qilishning asosiy qismi hisoblanadi. Serverlarning xavfsizligini ta’minlash tashkilotning umumiy kiberxavfsizlik strategiyasida ustuvor yo‘nalish hisoblanadi. Zamonaviy vositalardan foydalanish, xavfsizlik protokollarini amalga oshirish va muntazam monitoring orqali kiberjinoyatlarga qarshi samarali choralar ko‘rilishi mumkin. Shuningdek, xodimlarni xavfsizlik bo‘yicha o‘qitish va zaifliklarni muntazam tekshirish server xavfsizligini mustahkamlashga xizmat qiladi.

Foydalanilgan adabiyotlar ro‘yhati

1. Peter Szor “The Art of Computer Virus Research and Defense” 2005y
2. P.W. Singer, Allan Friedman “Cybersecurity and Cyberwar: What Everyone Needs to Know” 2014y
3. Andrew Magnusson “Practical Vulnerability Management: A Strategic Approach to Managing Cyber Risk” 2021
4. Chris Binnie “Linux Server Security: Hack and Defend” 2016y
5. Chris Sanders, Jason Smith “Applied Network Security Monitoring: Collection, Detection, and Analysis” 2013y

6. Heather Adkins, Betsy Beyer, Paul Blankinship “Building Secure and Reliable Systems” 2020y
7. Mike Chapple, David Seidl “CompTIA Security+ Study Guide” 2021y

KIBERJINOYATCHILIKKA QARSHI KURASHISHNING MUHANDISLIK-TEXNIK HOLATLARI

Boynazarov Otabek Murot o‘g‘li

IIV Malaka oshirish instituti, Axborot texnologiyalari sikli o‘qituvchisi
e-mail:boynazarovotabek0712@mail.ru

Kiberjinoyatchilik so‘nggi yillarda jahon miqyosida jiddiy xavf-xatarlarni keltirib chiqarayotgan global muammolardan biriga aylangan. Raqamli texnologiyalar va internet tarmoqlarining rivojlanishi bilan birga, kiberhujumlar va axborot xavfsizligiga tahdidlar ham ortmoqda. Kiberjinoyatchilik, insoniyatning axborot tizimlariga, shaxsiy ma'lumotlarga, moliyaviy resurslarga va davlat xavfsizligiga zarar yetkazish maqsadida amalga oshiriladigan jinoyatlarni o‘z ichiga oladi. Shu sababli, kiberjinoyatchilikka qarshi kurashish bugungi kunda texnologiya va muhandislik sohalarining dolzarb vazifalaridan biriga aylangan. Kiberjinoyatchilikka qarshi samarali kurashish uchun texnik va muhandislik yondashuvlari muhim ahamiyatga ega. Xavfsiz va ishonchli axborot tizimlarini yaratish, kiberhujumlarni aniqlash va ularga javob berish, tizimlarni himoya qilish va axborotlarni shifrlash kabi chora-tadbirlar kiberjinoyatchilikka qarshi kurashishda asosiy o‘rin tutadi. Ushbu ma’lumotlar, kiberjinoyatchilikning muhandislik-texnik holatlarini va shu sohada amalga oshirilishi lozim bo‘lgan chora-tadbirlarni yoritib, axborot xavfsizligi sohasida yuzaga keladigan eng muhim muammolarni tahlil qilishga qaratilgan.

Kiberjinoyatchilikka qarshi kurashishning muhandislik-texnik holatlari, texnologik va axborot xavfsizligi sohasidagi muammolarni hal qilishda muhim o‘rin tutadi. Quyidagi muhandislik-texnik holatlar kiberjinoyatchilikka qarshi kurashishda asosiy o‘rin tutadi:

- ***Kiberxavfsizlik tizimlari****:* Kiberjinoyatchilikka qarshi kurashishda kompyuter tarmoqlarining xavfsizligini taminlash uchun maxsus tizimlar yaratiladi. Ular, avvalo, tarmoq monitoringi, tarmoq trafigini tahlil qilish, xavfsizlik devorlari (firewall), antivirus dasturlar, shifrlash (encryption) va hujumlarni aniqlash tizimlari (IDS/IPS) kabi texnologiyalarni o‘z ichiga oladi.
- ***Axborotlarni shifrlash****:* Axborotlarni shifrlash kiberjinoyatchilar tomonidan ma'lumotlarni o‘g‘irlash yoki manipulyatsiya qilishni oldini olish uchun zarur. Bu texnologiyalar, masalan, AES (Advanced Encryption Standard), RSA, va TLS/SSL kabi protokollarni o‘z ichiga oladi.
- ***Himoya va avtonom tizimlar****:* Avtonom tizimlar (masalan, sun’iy intellekt va mashinani o‘rganish asosidagi tizimlar) hujumlarni prognoz qilish va oldini olishda yordam beradi. Kiberjinoyatchilikni aniqlashda algoritmlar va tizimlarning o‘rni katta.
- ***Xavfsizlik protokollari va autentifikatsiya****:* Foydalanuvchi va tizimlar o‘rtasida xavfsiz o‘zaro aloqani ta'minlash uchun autentifikatsiya protokollari (masalan, biometrik autentifikatsiya, ikki faktorli autentifikatsiya) joriy etiladi.

- ***Kiberhujumlarni tahlil qilish va javob berish:*** Kiberhujumga uchragan tizimlarni tahlil qilish, hujumning turi va manbasini aniqlash, hamda zararni kamaytirish uchun javob choralarini ko‘rish muhimdir. Bu jarayonda tizimlarning jurnalini tahlil qilish, rejalashtirilgan zararni minimallashtirish uchun kerakli choralarni ko‘rish zarur.
- ***Tarmoqni va serverlarni himoya qilish:*** Kiberjinoyatchilikka qarshi kurashish uchun tizimlarni va tarmoqlarni himoya qilish zarur. Bunga serverlarni yangilash, xavfsiz protokollarni qo‘llash, tarmoqdagi zaifliklarni aniqlash va ularni tuzatish kiradi.
- ***Ma’lumotlarni zaxiralash va tiklash:*** Kiberhujumlar va jinoyatchilar tomonidan tizimga zarar yetkazilgan hollarda, ma'lumotlarni tezda tiklash uchun zaxira nusxalari va tiklash jarayonlari joriy etiladi.
- ***Xavfsizlik siyosatlari va standartlar:*** Kiberjinoyatchilikka qarshi kurashishda tashkilotlarning xavfsizlik siyosatlari, qonunlar va xalqaro standartlarga rioya qilish muhimdir. Bunga ISO/IEC 27001, GDPR (General Data Protection Regulation) va boshqa xalqaro xavfsizlik standartlari kiradi.

Bu texnik chora-tadbirlar kiberjinoyatchilikka qarshi samarali kurashish va tizimlarning ishonchli ishlashini ta’minlashga yordam beradi. Samarali kiberxavfsizlikni ta’minlash uchun bir qator texnologik chora-tadbirlar, jumladan, tarmoqni himoya qilish, shifrlash, autentifikatsiya, va tizimlarni tahlil qilish zarur.
Kiberjinoyatchilikka qarshi kurashishda tizimlarni himoya qilish, xavfsizlik protokollarini joriy etish, ma’lumotlarni zaxiralash va tiklash kabi texnik yechimlar samarali ishlashini ta’minlashda muhim ahamiyatga ega. Bularning barchasi nafaqat individual foydalanuvchilar, balki butun jamiyat va davlat xavfsizligini ta'minlashga xizmat qiladi. Shuningdek, muhandislik va texnik yechimlarning muvaffaqiyatli ishlashi, kiberhujumlarni aniqlash va ularga javob berish, xavfsizlik siyosatlari va xalqaro standartlarga amal qilishni talab etadi. Kiberjinoyatchilikka qarshi kurashish uchun doimiy ravishda yangilanib turadigan texnologiyalar, chuqur tahlil va strategik yondashuvlar zarur. Kiberxavfsizlikni ta’minlashda mutaxassislar va barcha tizim ishtirokchilarining hamkorligi muhimdir. Faqatgina bunday yondashuv bilan kiberjinoyatchilikka qarshi samarali kurashish va axborot xavfsizligini ta’minlash mumkin.

Foydalanilgan adabiyotlar ro‘yhati

1. S. Harris “CISSP All-in-One Exam Guide. McGraw-Hill Education” 2021y.
2. R. Anderson “Security Engineering: A Guide to Building Dependable Distributed Systems” 2020y.
3. B. Qodirov & A. Raxmonov “Tarmoq xavfsizligi va kiberhujumlar” 2020y.
4. L. Zhang, & W. Lee “Internet of Things Security and Privacy*”* 2020y.
5. T. M. Chen & K. Wu “Cyber Security: Threats, Vulnerabilities, and Countermeasures” 2020y.
6. D. R. Kuhn, & D. Gollmann “Security in Computing” 2019y.
7. J. R. Vacca “Computer and Information Security Handbook” 2017*y.*

KIBERHUQUQ: RAQAMLI ASRDAGI HUQUQIY MUAMMOLAR VA ULARNING YECHIMLARI

Oripov Axmed Axtamovich

Ichki ishlar vazirligi ATAvaAHB katta muhandis-mutaxassisi

Kiberhuquq axborot-kommunikatsiya texnologiyalari sohasidagi munosabatlarni tartibga solishga va himoya qilishga qaratilgan huquq sohasidir. Kibermakon, axborot resurslari va tizimlari, raqamli iqtisodiyot va internetdagi intellektual mulk huquqlarining rivojlanishi bilan bog‘liq yangi munosabatlarning paydo bo‘lishi ushbu huquq sohasining zarurligini keltirib chiqardi [1].

Demak, kiberhuquq boshqa huquq sohalari qatorida o‘z ifodasini topgan yangi huquq tizimining elementi sifatida qaralishi kerak. Bu o‘z navbatida, mazkur huquq tarmog‘i bilan tartibga solinadigan munosabatlar, ularning obyekti, subyektlari hamda subyektlarning huquq va majburiyatlarini aniqlashtirishni taqozo etadi.

Kiberhuquqning huquqiy tartibga solish predmetiga kibermakonda yuzaga keladigan va turli huquq sohalarining normalari bilan tartibga solinadigan ijtimoiy munosabatlar majmui yoki yig‘indisi kiradi.

Kiberhuquqning asosiy vazifalari:

- *Kibermakondagi munosabatlarni huquqiy tartibga solish:* Bu vazifa jismoniy yoki yuridik shaxslarning kibermakondagi huquqlari va majburiyatlarini aniqlashtirishni, shuningdek, ushbu sohadagi faoliyatni tartibga soluvchi normalarni ishlab chiqishni o‘z ichiga oladi.
- *Kibermakondagi huquqlar va manfaatlarni himoya qilish:* Bu vazifa kiberjinoyatchilik, kiber-tajovuz, axborot xavfsizligi tahdidlari va boshqa zararli faoliyatlarga qarshi kurashishni o‘z ichiga oladi.

Kiberhuquq sohasidagi asosiy muammolar:

- *Yurisdiksiya:* Kibermakonning chegarasiz tabiati tufayli yurisdiksiya masalalari murakkablashadi. Jinoyatchilar va jabrlanuvchilar turli mamlakatlarda bo‘lishi mumkin, bu esa huquqni muhofaza qilish organlari uchun qiyinchiliklar tug‘diradi [2].
- *Maxfiylik va ma'lumotlarni himoya qilish:* Kibermakon shaxsiy ma'lumotlarni to‘plash, saqlash va ishlatish bilan bog‘liq muammolarni keltirib chiqaradi.

Qonunchilik shaxsning o‘z fikriga sobit bo‘lish huquqini mustahkamlaydi, ammo axborot tarqatish qonun asosida cheklanishi mumkin:

- ✓ *Kiberjinoyatchilik:* Kibermakon jinoyatchilar uchun yangi imkoniyatlar yaratadi. Zamonaviy texnologiyalar tufayli shaxslar o‘z uylaridan chiqmasdan ham jinoyat sodir etishmoqda [3].

✓ *Axborot xavfsizligi:* Kiberhujumlar davlatlar, tashkilotlar va shaxslar uchun jiddiy xavf tug‘diradi. Davlatlar kiberhujumlarga qarshi choralarni faqat qonun asosida amalga oshirishi lozim [3].

✓ *Huquqiy tartibga solishdagi kamchiliklar:* Kiberhuquq nisbatan yangi soha bo‘lib, qonunchilikdagi kamchiliklar va noaniqliklar tufayli yangi muammolarni keltirib chiqarishi mumkin. Masalan, O‘zbekiston qonunchiligida “aqidaparastlik” tushunchasi ishlatilsa-da, uning aniq mezonlari ko‘rsatilmagan [3].

Ushbu muammolarni hal qilish uchun quyidagi choralar ko‘rilishi mumkin:

✓ *Milliy qonunchilikni takomillashtirish:* Kiberhuquq sohasidagi milliy qonunchilikni takomillashtirish, xususan kiberjinoyatchilik, ma’lumotlarni himoya qilish, axborot xavfsizligi va boshqa dolzarb masalalarni tartibga soluvchi normalarni ishlab chiqish zarur. Qonunchilikdagi ziddiyatlar va noaniqliklar inson foydasiga talqin etilishi kerak [3].

✓ *Xalqaro hamkorlikni kuchaytirish:* Kiberhuquq sohasida xalqaro hamkorlikni kuchaytirish, jinoyatchilarni ta’qib qilish, dalillarni almashish va umumiy standartlarni ishlab chiqish uchun muhimdir [2].

✓ *Texnik choralarni qo‘llash:* Axborot tizimlarini himoya qilish, kiberhujumlarni aniqlash va oldini olish, shuningdek, kiberjinoyatchilikka qarshi kurashish uchun texnik choralarni qo‘llash zarur [1].

✓ *Jamiyatni xabardor qilish:* Kiberhuquq va kiberxavfsizlik masalalari bo‘yicha jamiyatni xabardor qilish, shuningdek, axborot texnologiyalaridan xavfsiz va mas’uliyatli foydalanishni targ‘ib qilish zarur.

Kiberhuquq doimiy rivojlanishda bo‘lgan sohadir. Yangi texnologiyalar, masalan, sun’iy intellekt, blokcheyn texnologiyasi va kvant hisoblash, yangi imkoniyatlar va tahdidlarni keltirib chiqaradi.

Kiberhuquq sohasidagi qonunchilik yangi texnologiyalarga moslashishi kerak. Bu esa, qonunchilikni takomillashtirish, xalqaro hamkorlikni kuchaytirish, texnik choralarni qo‘llash va jamiyatni xabardor qilish kabi choralarni o‘z ichiga oladi.

Kiberhuquqning kelajagi barcha manfaatdor tomonlarning birgalikdagi sa’y-harakatlariga bog‘liq. Davlatlar, xalqaro tashkilotlar kibermakonni xavfsiz, barqaror va inklyuziv qilish uchun birgalikda ishlashlari kerak.

Yuqorida keltirilgan muammolar va yechimlar kiberhuquq sohasining murakkabligini ko‘rsatadi. Ushbu sohadagi bilimlarni chuqurlashtirish va samarali siyosatlarni ishlab chiqish uchun doimiy tadqiqotlar hamda munozaralar olib borish lozim.

Foydalanilgan adabiyotlar ro‘yxati:

1. R.R. Shakurov, M.M. Vohidov. Kiberhuquq – huquq sohasi sifatida: risola. T:. 2022.
2. Kiberhuquq onlayn kurs. https://cyber-law.uz/uz/subject/kiber-huquq/
3. R. Eshboyev. Jamiyatni zararli axborotlardan himoya qilishda – inson huquqlari buzilmasligi kerak. Huquqshunosdan qonunchilikka tavsiyalar. https://m.kun.uz/news/2023/07/06/jamiyatni-zararli-axborotlardan-himoya-qilishda-inson-huquqlari-buzilmasligi-kerak-huquqshunosdan-qonunchilikka-tavsiyalar?q=%2Fuz%2Fnews%2F2023%2F07%2F06%2Fjamiyatni-zararli-axborotlardan-himoya-qilishda-inson-huquqlari-buzilmasligi-kerak-huquqshunosdan-qonunchilikka-tavsiyalar

ZAMONAVIY KIBERJINOYAT XAVFLARI VA ULARNING OLDINI OLISH

A.A.Abdiraximov

IIV Malaka oshirish instituti, Axborot texnologiyalari sikli o‘qituvchisi, katta leytenant e-mail: amr.herezen28@gmail.com tel:+998944282802

Annotatsiya: *Mazkur maqolada Kiberjinoyatlar zamonaviy texnologiyalar rivoji bilan birgalikda ko‘payib bormoqda. Ushbu maqola zamonaviy kiberjinoyat turlarini, ularning ishlash mexanizmlarini va foydalanuvchilar hamda tashkilotlarga etkazishi mumkin bo‘lgan zararlarini yoritadi. Asosiy urg‘u kiberjinoyatchilikning quyidagi turlariga qaratilgan: farming (DNS hujumlari orqali soxta saytga yo‘naltirish), kiberxavfsizlikning dolzarbligini ta’kidlab, texnologiyalar bilan bog‘liq xavf-xatarlarni kamaytirishga oid strategiyalarni taklif qiladi.*

Kalit so‘zlar: *Farming, ransomware, kiberxavfsizlik, DNS hujumlari, ma’lumotlarni himoya qilish.*

Texnologiyalar rivoji bilan kiberjinoyatchilik usullari ham takomillashmoqda. Zamonaviy xavfsizlik tizimlari rivojlangan bo‘lsa-da, kiberjinoyatchilar yangi va ilg‘or usullarni qo‘llab, foydalanuvchilarga zarar yetkazishda davom etmoqda. Ulardan biri – farming (yoki pharming) texnikasi. Ushbu maqolada farming orqali kiberjinoyatlar, ularning ishlash mexanizmi va ulardan himoyalanish yo‘llari haqida so‘z boradi.

Farming (pharming) nima?

Farming – kiberjinoyatchilikning zamonaviy usuli bo‘lib, foydalanuvchi haqiqiy veb-saytga o‘xshash soxta saytga yo‘naltiriladi. Ushbu jarayonda jinoyatchilar foydalanuvchining shaxsiy ma’lumotlarini, jumladan, login va parollarni, bank rekvizitlarini yoki boshqa maxfiy ma’lumotlarni qo‘lga kiritadi.

Masalan, *https://click.uz* bu sayt O‘zbekiston hududidan ro‘yxatdan o‘tgan, uz domenidagi click kompaniyasining haqiqiy saytidir. Bunday domenda umuman sayt ochib bo‘lmaydi. Firibgarlar bu saytni tashqi tarafdan bir xil qilib, sizni click.uz saytiga o‘ting deb havola qoldirgani bilan, sizning brauzeringizda *click.space* nomli boshqa

domen chiqishi mumkin. Shunday qilib, siz soxta saytlarni ajratib olishingiz mumkin. To‘lovlarni amalga oshirishda va plastik karta ma’lumotlaringizni kiritayotganingizda saytning domeniga e’tiborli bo‘ling. [1]

DNS hujumlari (DNS Spoofing) – Kiberjinoyatchilar DNS tizimini buzib, haqiqiy sayt domenini soxta saytga yo‘naltiradi. Masalan, foydalanuvchi bank sayti URL manzilini kiritadi, lekin jinoyatchilar tomonidan yaratilgan soxta bank saytiga kiradi. Kompyuter yoki qurilmaga o‘rnatilgan zararli dastur (malware) tarmoq sozlamalarini o‘zgartiradi va foydalanuvchini avtomatik ravishda jinoyatchilar saytiga yo‘naltiradi. Brauzer xatolari (man-in-the-middle attack): Jinoyatchilar foydalanuvchi va haqiqiy sayt orasidagi aloqa kanaliga o‘rnashib, ma’lumotlarni soxta saytga o‘zgartiradi.

Farmingning maqsadi kiberjinoyatchilar farming usulidan quyidagi maqsadlarda foydalanadi:

- ❖ Moliyaviy foyda olish: Foydalanuvchilarning bank hisob raqamlari yoki kartalari ma’lumotlarini o‘g‘irlash.
- ❖ Identifikatsiyani o‘g‘irlash: Login, parol yoki shaxsiy ma’lumotlarni qo‘lga kiritish.
- ❖ Tarmoq infratuzilmasiga zarar yetkazish: Tizimni yo‘q qilish yoki zararli dasturlarni tarqatish.

Farmingning real hayotdagi misollar: Bank xizmatlariga hujumlar: Jinoyatchilar odamlarni bank saytlariga o‘xshash soxta sahifalarga yo‘naltiradi va parol hamda hisob ma’lumotlarini o‘g‘irlaydi. Ijtimoiy tarmoqlar: Mashhur platformalar (masalan, Facebook yoki Instagram) soxta sahifalar yaratilib, foydalanuvchi ma’lumotlari o‘g‘irlanadi. E-tijorat saytlariga hujum: Xaridorlar soxta sahifalarga yo‘naltirilib, ular tomonidan kiritilgan to‘lov ma’lumotlari jinoyatchilar qo‘liga tushadi.

Farmingdan himoyalanish yo‘llari kiberjinoyatlardan himoyalanish uchun quyidagi choralarni ko‘rish zarur:

1. DNS xavfsizligini mustahkamlash. Tizimni yangilab turish va DNS himoya vositalaridan foydalanish.
2. SSL sertifikatlarini tekshirish. Saytlarga kirishda, URL manzilida “https://” prefiksiga e’tibor bering va qulf belgisini tekshiring.
3. Zararli dasturlarga qarshi dasturiy ta’minot. Kompyuter va qurilmalarni antivirus va antimalware vositalari bilan himoya qiling.
4. Shubhali xabar va havolalardan ehtiyot bo‘ling.Elektron pochta yoki SMS orqali kelgan noma’lum havolalarga bosilgandan saqlaning.
5. Ikkilik autentifikatsiyadan foydalaning Login jarayonida qo‘shimcha xavfsizlik qatlamini qo‘shish orqali ma’lumotlaringizni himoyalang.

Xulosa. Farming texnikasi zamonaviy kiberjinoyatchilikning samarali usuli bo‘lib, uning oqibatlari jiddiy bo‘lishi mumkin. Foydalanuvchilar xavfsizlik choralarini ko‘rib, internetdan foydalanishdagi xabardorlikni oshirishlari lozim. Texnologik yutuqlar bilan birga xavf-xatarlar ham ko‘paymoqda, shuning uchun raqamli dunyoda ehtiyotkor bo‘lish dolzarb masaladir. Shimoliy Koreya bilan bog‘liq “Kimsuky” guruhi hozirda hisob ma’lumotlarini o‘g‘irlashga qaratilgan fishing hujumlarini yashirish uchun “Mail ru” kabi rus elektron pochta xizmatlaridan foydalanmoqda.

Eslatma: Agar siz kiberjinoyatchilikning qurboni bo‘lsangiz, darhol maxsus xizmatlarga murojaat qiling va muammolar haqida xabar bering.

Foydalanilgan adabiyotlar ro‘yhati:

1. U.Sh.Xamroqulov, J.D.Risqaliyev, Sh.E.Sheraliyev, O.M.Boynazarov Kiberxavfsizlik asoslari (Ichki ishlar organlari uchun uslubiy qo‘llanma). – T.: IIV MOI, 2022. – 63 b.
2. Goodman, M. (2015) – Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. Anchor Books.
3. Zav’yalov S. International experience in fighting the propaganda of terrorism in the Internet. Zarubezhnoevoennoeobozrenie = Foreign Military Review, 2014, no. 4, pp. 34–39. (In Russian).
4. https://thehackernews.com/2024/12/north-korean-kimsuky-hackers-use.html.

КИБЕРЖИНОЯТЛАРНИ ИСБОТЛАШДА МАСОФАВИЙ ТЕРГОВ ҲАРАКАТЛАРИНИНГ ЎРНИ

Файзуллаев Шавкат Файзуллаевич

Аннотация: Ушбу мақолада кибержиноятчиликка қарши курашиш борасида жиноят ишларини тергов қилиш, юзага келаётган ҳуқуқий муаммолар, олис ҳудуддаги кибержиноят қуробонлари билан боғлиқ тергов ҳаракатларини видеоконференцалоқа режимида ўтказиш, амалиётда кузатилаётган ноқулайликлар, мазкур режимнинг суриштирув ва тергов органлари томонидан оммалашмаётганлиги сабаблари, бу борада илғор хорижий давлатларнинг қонунчилиги ютуқлари, ишлаш меҳанизмларини такомиллаштириш борасида чет эл олимларининг мулоҳазалари ҳар томонлама таҳлил этилиб, қонунчиликкка энг мақбул келадиган таклифлар илгари сурилган ҳамда тўлиқ амалиёт нуқтаи назаридан асослантирилиб, илмий хулосаларга келинган.

Калит сўзлар: кибержиноят, видеоконференцалоқа, масофавий тергов ҳаракатлари, электрон ҳукумат, рақамли иқтисодиёт, киберҳужум, жамиятни ахборотлаштириш.

Жамият ривожланган сари, ундаги ижтимоий муносабатлар ҳам мураккаблашиб боради. Бундай муносабатлардан бири, киберхавсизлик соҳасидаги муносабатлардир.

Электрон ҳукумат, рақамли иқтисодиёт, жамиятни ахборотлаштириш, IT-таълим... Буларнинг барчаси айни замонамизда оммалашиб улгурди. Бир сўз билан айтганда, дунё рақамлашмоқда. Яқинда SEON компанияси киберхавфсизлик рейтингини тақдим этди. Рейтингига кўра, Дания киберхавфсизлик бўйича энг юқори кўрсаткичга эга. Ушбу мамлакатда одамлар кибержиноятлардан қонунчилик ва технология орқали энг яхши ҳимояланган. Ундан сўнг рўйхатда Германия ва АҚШ ўрин олган. [1.]

2024 йил май ойида Ўзбекистоннинг “uz” домен веб-сайтларига 6,6 миллиондан ортиқ киберҳужумлар амалга оширилди. Технологиялар даврида

жиноятчилар пул маблағлари, махфий маълумотларга ўз шахсларини ошкор қилмасдан тўғридан-тўғри фойдаланиш ва шу билан бирга анонимликни сақлаб қолиш имконига эга. Кибертаҳдидлар сони ўсиб бораётган бир вақтда, ушбу жиноятларнинг олдини олиш учун ахборот хавфсизлиги ёки киберхавфсизлик соҳа вакиллари жадал кураш олиб бормоқда. Аммо, шунга қарамасдан 2021-2023 йилларда Ўзбекистонда кибержиноятлар сони 25 бараварга ошгани.[1.] Шу сабабли ҳам 2022 йилда “Киберхавфсизлик тўғрисида”ги Қонун ҳам қабул қилинди.[2.] Натижада киберхавфсизлик соҳасидаги муносабатлар қонун билан тартибга солинди.

Кибержиноятлар ошиши билан бирга, мазкур турдаги жиноятларни содир этган шахсларни айбини исботлаш, жавбрланувчилар доирасини аниқлаш, зарар миқдорини ҳисоблаш масалалари ҳам кун тартибига чиқди. Барчамизга маълумки, кибержиноятчилар учун масофанинг ахамияти йўқ. Одатда жабрланувчилар бир биридан узоқ ҳудудларда истиқомат қилишса, кибержиноятчилар чет элда туриб қинғир ишларини амалга ошириши ҳам мумкин. Мазкур мураккаб вазиятда узоқ ҳудудда яшовчи процесс иштирокчилари билан боғлиқ тергов ҳаракатлари ўтказилишини тақазо этади.

Дастлаб, Ўзбекистонда иқтисодий ва фуқаролик ҳуқуқий муносабатларида видеоконференцалоқадан фойдаланиш амалиёти бирмунча олдинроқ бошланган бўлсада, 2018 йил 18 апрелдаги “Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартиш ва қўшимчалар киритиш тўғрисида”ги ЎРҚ-476-сон [4.] Қонуни билан биринчи маротаба жиноят-процессуал қонунчилигига видеоконференцалоқадан фойдаланиш тартиби мустаҳкамланди. Том маънода жиноят процессида ахборот технологияларидан фойдаланиш ҳам шу даврда бошланди.[5.] Дастлаб, видеоконференцалоқадан фойдаланиш ваколати фақат судларга берилган бўлиб, бугунги кунда суриштирув, давтлабки тергов органларига ҳам дилаллар тўплаш вақтида фойдаланиш ваколати мустаҳкамлаб қўйилди.

Кибержиноятлар юзасидан мамлакат ичкарисида амалга ошириладиган тергов ҳаракатлари билан бир қаторда жиноят иши доирасида ҳорижий давлатлар ҳудудида ҳам тергов ҳаракатларини ўтказишга эҳтиёж сезилади. Бу эҳтиёж айниқса глобаллашув жараёнида кучайиши кузатилмоқда. Ўрганиш давомида тергов органи томонидан фуқаро М.А.га нисбатан қўзғатилган жиноят иши доирасида ягона гувоҳ 2024 йилнинг май ойида, терговга қадар текширув тугамасиданоқ меҳнат мухожири сифатида Туркия Республикасига кетганлиги маълум бўлган. Афсуски у билан боғлиқ далилларни олиш муаммога айланган. Халқаро ҳамкорлик борасида сўров юбориш эса узоқ муддатли жараён ҳисобланади. Амалдаги ЖПКмизга халқаро амалиётда эътироф этилган жиноят-ҳуқуқий институтларнинг етарли даражада имплементация қилинмаганлиги Президентимиз томонидан ҳам қайд этилган. [6.] Шу билан бирга, баъзи

тадқиқотчилар миллий қонунчиликда тўғридан тўғри хориждаги шахслар билан масофавий тергов ҳаракатларини ўтказиш назарда тутилмаган бўлсада анология бўйича шахс ҳуқуқларини таъминлаш учун ўтказиш мумкин [7.] деган хулосага келишган. А.С.Климантъев [8.] ҳам халқаро ҳамкорлик борасида видеоконференцалоқадан фойдаланиш энг мақбул вариант эканлигини қайд этади. Жиноят иши доирасида мамлакатлар ўртасида амалга ошириладиган алоқалар халқаро, минтақивий ва икки томонлама тузилган шартномаларга шунингдек, ўзаролик принципига асосланилади. Бундай вазиятда энг мақбул йўл ўзаро ҳуқуқий ёрдам сўраб мурожаат қилиш ҳисобланади. [9.] Мазкур масалаларни тартибга солиш икки томонлама, минтақавий даражада ривожланади.

Сўнги 30 йилда халқаро муносабатлар доирасида видеоконференцалоқадан фойдаланишни тартибга солувчи халқаро ҳужжатлар сони ортиб бориш тенденцияси кузатилди. Халқаро миқёсда биринчи маротаба жиноят процессида далилларни тақдим этиш учун видеоконференцалоқадан фойдаланишнинг мақбуллиги 1990 йилда “Жиноят ва ҳокимиятни суиистеъмол қилиш қурбонлари учун Одил судловнинг асосий тамойиллари тўғрисида”ги Декларациясида белгиланган.[10.] Халқаро шартномаларнинг аксар қисми жиноят иши юзасидан халқаро ҳуқуқий ёрдам кўрсатиш борасида видеоконференцалоқадан фойдаланиш тартибини белгилаб берган. Шундай қилиб, 2000 йил 15 ноябрдаги БМТнинг Трансмиллий уюшган жиноятчиликка қарши Конвенсиясининг [11.] 18-моддаси 18-бандида видеоалоқа қўллаш ҳақида ваколат берилган бўлиб, унга кўра гувоҳ сифатида битта давлат ҳудудида бўлган гувоҳни ёки экспертларни видеоконференцалоқа орқали сўроқ қилиш мумкинлиги кўрсатилган. Мазкур Конвенция Ўзбекистон томонидан ратификация қилинган. [12.] Шу каби қоидалар Кишинёв Конвенциясида [13.] ҳам мавжуд.

Энди эса видеоконференцалоқадан фойдаланишни тартибга солиш юзасидан айрим хорижий давлатларнинг жиноят иши бўйича ўзаро ҳуқуқий ёрдам кўрсатиш борасидаги белгиланган қоидаларини кўриб чиқамиз.

Жиноят ишлари бўйича ҳуқуқий ёрдам кўрсатишда видеоконференцалоқадан фойдаланишнинг процессуал тартиби Эстония Жиноят-процессуал кодексининг 19-бобида мустаҳкамланган бўлиб, хорижда масофавий тергов ҳаракатлари ўткази ва дилиллар тўплаш, олинган далилларнинг мақбуллиги масаласи ёритилган. Канада ҳам ҳорижда бўлган процесс иштирокчилари билан боғлиқ тергов ҳаракатларини ўтказишда алохида қоидалар белгиланган [14.] ва “Жиноят ишлари бўйича ўзаро ҳуқуқий ёрдам тўғрисида”ги [15.] қонунларига кўра, масофавий гувоҳлик бериш имконияти берилган.

Бизнинг ЖПКда бўлгани каби Россияда ҳам айнан жиноят иши бўйича ўзаро ҳуқуқий ёрдам борасида видеоконференцалоқадан фойдаланиш тартиби аниқ белгиланмаганлиги айрим олимлар томонидан қайд этилади. Бу борада З.А.Тлехучнинг қайд этишича, Россия Федерацияси Жиноят-процессуал кодексида ишни судга қадар юритиш босқичида видеоконференцалоқадан фойдаланишнинг ҳуқуқий асослари мавжуд эмаслиги жиноят ишлари бўйича ўзаро ҳуқуқий ёрдам кўрсатиш борасидаги сўровларни ўз вақтида бажариш

имкониятини камайтиради. [16.] М.И.Смирновнинг қарашларига кўра, бугун далилларни чет элдан қисқа муддатларда ва сифатли олиш механизми бўлиши кераклиги сабабли бу ролни видеоконференцалоқа самарали бажаради. [17.] Халқаро алоқаларда видеоконференцалоқанинг фойдаланилиши топшириқларни ўз вақтида ва сифатли бажарилишига хизмат қилади. [18.] Бундан англаш мумкинки, ички қонунчиликда ҳам халқаро хамкорлик соҳасида видеоконференцалоқадан фойдаланиш тартиби мустаҳкамланган бўлиши зарур. Бу каби қоидалар Озорбойжон,[19.] Грузия,[20.] Қозоғистон, [21.] Латвия, [22.] Қирғизистон, [23.] Украина, [24.] Эстония, [25.] қонунчилигида ҳам белгиланган. Бизнинг қонунчилигимизда эса суриштирув ва дастлабки тергов ҳамда суд жараёнида мазкур тергов ҳаракатларини ўтказиш режимини қўллаш имконияти қонун билан мустаҳкамланган бўлсада, аммо жиноят иши юзасидан амалга ошириладиган ўзаро ҳуқуқий ёрдам доирасида видеоконференцалоқадан фойдаланиш тартиби ЖПКда назарда тутилмаган. Мазкур муаммога С.С.Орипов [26.] ҳам тўхталиб, процессуал ҳаракат ўтказилиши лозим бўлган шахснинг хорижий давлат ҳудудида бўлган ҳолатларни қайд этади. Афсуски, ЖПКда мазкур ҳолатда қандай ҳаракат қилиш назарда тутилмаган. Мисол учун, жиноят иши бўйича асосий фигурант бўлган гувоҳ ёки жабрланувчи чет элда бўлганда у билан ишнинг янги аниқланган ҳолатларига ойдинлик киритиш мақсадида ўтказилиши лозим бўлган масофавий тергов ҳаракатини видеоконференцалоқа режимида ўтказишга ЖПК рухсат бермайди.

Юқорида жиноят иши доирасида амалга ошириладиган халқаро муносабатлар ва ҳамкорлик борасида хорижий давлатларнинг тажрибалари ўрганилиб, миллий қонунчилигимиз билан таққосланди. Натижада эса миллий қонунчилигмизда мавжуд бўлган бўшлиқлар ва тўлдирилиши лозим бўлган тузатишлар яққол кўзга ташланади. Мисол учун Ўзбекистон Республикаси Жиноят-процессуал кодексида хам жиноят иши юзасидан халқаро ҳамкорликка алохида боб ажратилган бўлсада айнан хорижий давлат билан боғлиқ масофавий тергов ҳаракатларини ўтказиш тартиби, сўроқ, нарса ва буюмларни таниб олиш учун кўрсатиш, юзлаштириш ва бошқа тергов ҳаракатларини видеоконференцалоқа режимида ўтказишга бағишланган тартиб қоидалар мавжуд эмас. Юқорида қонунчилиги ўрганилган давлатларда эса мазкур тартиблар алохида модда шаклида кўрсатиб ўтилган. Халқаро муносабатларда бу каби тартибларни аниқ қилиб мустаҳкамлаб қўйилиши эса юзага келиши мумкин бўлган баҳсли масалаларга барҳам беради. Баъзи ўрганилган давлатларнинг қонунчилигида видеоконференцалоқадан фойдаланиш умумий тартибда халқаро алоқаларда ҳам қўлланилиши киритиб ўтилган.

Миллий қонунчилигмизни таҳлил қилиб, унга баъзи тузатишлар киритилиши ҳақида асослантирилган хулосага келинади. Жумладан ЖПКнинг 91^2-моддасида тергов ҳаракатларини видеоконференцалоқа режимида ўтказишнинг 4 та асоси баён қилинган. Аммо хорижий давлатларнинг қонунчилигида жиноят иши доирасида амалга ошириладиган ўзаро ҳуқуқий ёрдам борасида ҳам видеоконференцалоқадан фойдаланиш асоси айнан шу моддада келтирилганлигини кўриш мумкин. Мисол учун Озорбойжон Республикаси Жиноят-процессуал кодексининг 52-2-моддасида [27.] айнан

видеоконференцалоқа режимида тергов ҳаракатлари ўтказиш тартиби мустаҳкамланган модданинг ўзидаёқ хорижий давлат ҳудудида бўлган процесс иштирокчиси билан боғлиқ масофавий тергов ҳаракталарини ўзаро ҳуқуқий ёрдам кўрсатиш мумкинлиги кўрсатилган. Жиноят процессуал қонунчилиги ўрганилган Қозоғистон, Латвия, Қирғизистон, Украина ва бошқа давлатларда тергов ҳаракатларини видеоконференцалоқа режимида ўтказиш тартиб - қоидалари белгиланиши билан бирга, жиноят иши доирасида ўзаро ҳуқуқий ёрдам масаласида ҳам видеоконференцалоқа режимини қўллаш тартиби, хорижий давлатдан масофавий тергов ҳаракатлари натижасида олинган далилларнинг мақбуллиги ҳақида қоидалар мустаҳкамланган. Ўтказилган сўровнома натижасига кўра, респондентларнинг қарийб 46% фаолиятида хорижда бўлган процесс иштирокчилари билан боғлиқ масофавий тергов ҳаракатини ўтказишга эҳтиёж сезганлигини ва ЖПКга киритилиши зарурлигини билдиришган. [28.] Шу сабабли ҳам 91^2-моддасига 5-асос сифатида “жиноят иши доирасида судлар, прокурорлар, терговчилар ва суриштирув органларининг хорижий давлатлар ваколатли органлари билан ўзаро ҳамкорлигини амалга оширишда” деб қўшимча киритиш лозим бўлади.

Бундан ташқари, Ўзбекистон ЖПКда 14-бўлим (2-та боб, 17 та модда) халқаро ҳаморклик масалаларига бағишланган бўлсада, Ўзбекистон Республикаси ҳудудидан ташқарида бўлган гувоҳни, жабрланувчини, экспертни, фуқаровий даъвогарни, фуқаровий жавобгарни, уларнинг вакиллари ҳамда процесснинг бошқа иштирокчиларини видеоконференцалоқа орқали сўроқ қилиш тартиби киритилмаган. Жиноят ишларини ўрганиш натижасида ЎзР ЖКнинг 168-моддаси 3-қисми “б” банди билан қўзғатилган жиноят иши юзасидан фуқаро Б.О. РФда бўлиб, дастлаки тергов органи билан телефон орқали гаплашиб турганлиги, жиноят иши доирасида юборилган сўровнома жавоби келиши кўп вақт талаб этганлиги сабабли ва дастлабки тергов муддатини тежаш мақсадида жиноят иши ЖПКнинг 364-моддаси 1-қисми 1-банди (иш бўйича айбланувчи тариқасида иштирок этишга жалб қилиниши лозим бўлган шахс аниқланмаган) асоси билан тўхтатилганлиги маълум бўлди. Иш ҳужжатларида эса РФ ваколатли органлари қарийб 2 ой илгари сўровнома юборилган. Бу каби жиноят ишларини Республика доирасида кўплаб учратиш мумкин. Шу сабабли ҳам ЖПКга қўшимчалар киритилиб, халқаро ҳамкорлик доирасида тергов ҳаракатларини видеоконференцалоқа режимида ўтказиш тартиби аниқ белгиланиши, мазкур режим орқали олинган далилларнинг мақбуллиги масалаларига ойдинлик киритиш лозим бўлади. Натижада эса олис мамлакатда бўлган процесс иштирокчилари билан боғлиқ тергов ҳаракатларини ўтказишнинг ҳуқуқий асоси мустаҳкамланади. Бу эса кибержиноятларни исботлаш самарадорлигини ошишига хизмат қилади.

АДАБИЁТЛАР РЎЙХАТИ:

1.Таҳлил: Кибержиноятчилик: хавфга қанчалик тайёрсиз? http://m.xabar.uz/post/kiberjinoyatchilik-xavfga-qanchalik-tayyorsiz?category=tahlil

2.Ўзбекистонда кибержиноятчилик муаммоси: ҳужумлар сони 25 бараварга ошди. https://daryo.uz/k/2024/08/27/ozbekistonda-kiberxavfsizlik-muammosi-hujumlar-soni-25-baravarga-oshdi
3.“Киберхавфсизлик тўғрисида”ги ЎРҚ-764-сон Қонун. (Қонунчилик маълумотлари миллий базаси, 16.04.2022 й., 03/22/764/0313-сон) https://lex.uz/uz/docs/5960604
4.https://lex.uz/uz/docs/3689258 (мурожаат вақти 29.11.2022 й)
5.С.С.Орипов- Ишни судга қадар юритиш босқичида ахборот технологияларидан фойдаланишни такомиллаштириш. Дисс. Phd. Б-36. Т.,2023 йил
6.Ўзбекистон Республикаси Президентининг қарори ПҚ-3723-сон. – “Жиноят ва жиноят-процессуал қонунчилиги тизимини тубдан такомиллаштириш чора-тадбирлари тўғрисида”. 2018 йил 14 май. https://lex.uz/docs/3735818 (мурожаат вақти 20.05.2024 йил.)
7.Рамазанов Рамиль Миргаязович. Деятельность суда по обеспечению безопасности участников уголовного процесса. Автореферат диссертации на соискание ученой степени кандидата юридических наук. Ульяновск - 2022.-С-11
8.Клементьев Александр Станиславович. Телекоммуникационное обеспечение уголовного процесса. Автореферат диссертации на соискание ученой степени кандидата юридических наук. Владимир-2007.С-9.
9.Сахаддинов Солоҳиддин. Ўзбекистон Республикасининиг Жиноят-процессуал кодексига шархлар: махсус қисм / Масъул муҳаррир Б.Х.Пўлатов. - Тошкент: Янги аср авлоди, 2014. Б-246
https://drive.google.com/file/d/13vvbCAdxiZpMydTywJbsy9mtsmHavVL5/view
10.Архипова Екатерина Александровна. Применение видеоконференцсвязи в уголовном судопроизводстве России и зарубежных стран: сравнительно-правовое исследование: Дисс.канд. юрид. наук. –Москва-2013. С-104.
11. Конвенция Организации Обьединенных Наций против транснациональной организовонной приступности. Ўзбекистон Республикасининг халқаро шартномалари тўплами 2004 йил. 1-сон
12. Бирлашган Миллатлар Ташкилотининг Трансмиллий уюшган жиноятчиликка қарши Конвенциясини ратификация қилиш тўғрисида 2003 йил 30 август, 536-II-сон Олий Мажлис қарори. (мурожаат вақти 07.06.2023 йил) https://lex.uz/docs/1328107
13. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (Кишинев, 7 октября 2002 года). (мурожаат вақти 29.05.2023 йил) https://base.garant.ru/10119702/
14.CANADA EVIDENCE ACT. R.S.C., 1985, c. C-5. (мурожаат вақти 25.06.2023 йил) Канадский закон о доказательствах (justice.gc.ca)
15.Закон о взаимной правовой помощи по уголовным делам Канады. R.S.C., 1985, c. 30 (4th Supp.) (мурожаат вақти 26.06.2023 йил) Закон о взаимной правовой помощи по уголовным делам (justice.gc.ca)
16.Тлехуч Заурбий Азметович.- Собирание доказательств по уголовным делам на территориях иностранных государств при оказании правовой помощи. Автореферат диссертации на соискание ученой степени кандидата юридических наук. Москва-2021г. Б-55. Автореферат Тлехуч З.А..pdf (agprf.org)

17.М.И.Смирнов, Эффективность механизмов и процедур оказания взаимной правовой помощи по уголовным делам: вопросы процессуальной формы. С-6 Эффективность механизмов и процедур оказания взаимной правовой помощи по уголовным делам: вопросы процессуальной формы (sovremennoepravo.ru)
18.Нурбеков Искендер Маликович. Тактико-организационные особенности взаимодействия при расследовании преступлений международного характера. Автореферат диссертации на соискание учёной степени кандидата юридических наук. М.-2010. С-27.
19.Azərbaycan Cinayət Prosessual Məcəlləsi. (Bu Məcəllə Azərbaycan Respublikasının 2000-ci il 14 iyul tarixli 907-IQ nömrəli Qanunu ilə təsdiq edilmişdir). (мурожаат вақти 29.07.2023 йил). https://www.e-qanun.az/framework/46950#_edn1
20.Уголовно-процессуальный кодекс Грузии. Консолидированный публикации 15.06.2023 г. (мурожаат вақти 31.07.2023 йил). https://matsne.gov.ge/ru/document/view/90034?publication=151
21.Қазақстан Республикасының Қылмыстық іс жүргізу кодексі. (мурожаат вақти 01.08.2023 йил) https://adilet.zan.kz/kaz/docs/Z970000206
22.Уголовно-процессуальный закон Латвийской Республики принятый Сеймом 21 апреля 2005 года. (мурожаат вақти 02.08.2023 йил). https://lawyer-khroulev.com/zakoni-kodeksi-latvii-i-germanii/v - Законы Латвии по-русски
23.КЫРГЫЗ РЕСПУБЛИКАСЫНЫН КЫЛМЫШ-ЖАЗА ПРОЦЕССУАЛДЫК КОДЕКСИ. 2021-жылдын 28-октябры № 129 *(Кыргыз Республикасынын 2021-жылдын 28-октябрындагы № 126 Мыйзамы менен колдонууга киргизилди)* (мурожаат вақти 02.08.2023 йил). http://cbd.minjust.gov.kg/act/view/ky-kg/112308
24.Уголовный процессуальный кодекс Украины от 13 апреля 2012 года № 4651-VI (с изменениями и дополнениями по состоянию на 21.03.2023г.) (мурожаат вақти 03.08.2023 йил). https://continent-online.com/Document/?doc_id=31197178#pos=5;-128&sdoc_params=text%3D%25D0%25B2%25D0%25B8%25D0%25B4%25D0%25B5%25D0%25BE%26mode%3Dindoc%26topic_id%3D31197178%26spos%3D1%26tSynonym%3D0%26tShort%3D1%26tSuffix%3D1&sdoc_pos=5
25.Уголовно-Процессуальный Кодекс Эстонии принят 12.02.2003 RT I 2003, 27, 166. (мурожаат вақти 05.08.2023 йил)
https://www.wipo.int/wipolex/ru/legislation/details/1291
26. Уша манба: С.С.Орипов - Ишни судга қадар юритиш босқичида ахборот технологияларидан фойдаланишни такомиллаштириш. Дисс. Phd. Б-36. Т.,2023 йил
27.Azərbaycan Cinayət Prosessual Məcəlləsi. (Bu Məcəllə Azərbaycan Respublikasının 2000-ci il 14 iyul tarixli 907-IQ nömrəli Qanunu ilə təsdiq edilmişdir). (мурожаат вақти 29.07.2023 йил). https://www.e-qanun.az/framework/46950#_edn1
28. Уша манба: С.С.Орипов - Ишни судга қадар юритиш босқичида ахборот технологияларидан фойдаланишни такомиллаштириш. Дисс. Phd. Б-36. Т.,2023 йил.

КИБЕРЖИНОЯТЛАРНИ ТЕРГОВ ҚИЛИШДА РАҚАМЛИ ЭКСПЕРТИЗАНИНГ ЗАРУРАТИ

Раджапов Олимбой Эркаевич

Хоразм вилояти ИИБ Эксперт-криминалистика маркази бошлиғи

Аннотация: Мақолада кибержиноятларни очиш ва тергов қилишда рақамли экспертизадан фойдаланишнинг аҳамиятли томонлари, рақамли экспертизага тақдим этилиши лозим бўлган объектлар ва уларни ҳодиса жойини кўздан кечиришда аниқлаш, олиш ва қайд этиш тартибларига оид фикр ва мулоҳазалар билдирилган.

Калит сўзлар: *рақамли экспертиза, компьютер, техника воситалари, технология, далиллар, ахборот манбалари, кибержиноятлар, илмий метод, таҳлил.*

Бугунги кунда технологияларнинг тезкор ривожланиши оқибатида жиноятларнинг ҳам янги кўринишлари пайдо бўлмоқда. Илдамлик билан ривожланаётган жиноят тури бўлган кибержиноятлар бутун дунё бўйлаб тарқалаётган трансмиллий таҳдидга айланди.

Мазкур жиноят тури тўсиқ ва чегараларни билмайди. Ёши, келиб чиқиши, яшаш жойидан қатъи назар, ҳар ким кибержиноятлар қурбони бўлиши мумкин. Онлайн-жиноятларнинг трансмиллийлиги, миқёси ҳамда экстерриториал рақамли далилларнинг мавжудлиги кибержиноятларни тергов қилишда мутахассислардан махсус билимларни талаб қилади.

Ўзбекистонда эндигина ташкил қилинган ва жиноятларни очишда қўлланила бошланган экспертиза турларидан бири бўлган рақамли экспертиза истиқболдаги тадрижий юқори натижадорликни кўрсатувчи экспертизага айланиши муболағасиз муҳим омил саналади [1]. Дунё аҳолисининг кўпчилиги телефон орқали муомала қилиши, иш фаолияти ёки ўқиш жараёнлари ҳам айнан онлайн тизимга ўтганлиги, ҳужжатлар айланишидан тортиб маълумотлар алмашинуви ҳам ахборот технологиялари орқали амалга оширилишининг оммавийлашиши, компьютердан фойдаланиш янгилик эмаслиги барчамизга аён. Шунингдек, шахслар турли маълумот ташувчи воситаларда ўз муҳим маълумотларини сақлайди. Мадомики шундай экан, ахборот технологиялари соҳасидаги жиноятлар содир этилган тақдирда, жиноятларни очишда ушбу маълумотларни топа олиш, тиклай олиш, улардан жиноятларни очиш жараёнида фойдаланиш муҳим саналади. Хусусан, бугун рақамли далиллар билан ишлаш жараёнида судга қадар ва суд муҳокамаси босқичларида ғоят аҳамиятни касб этади. Сабаби, рақамли далиллар билан ишлаш суриштирувчи-терговчидан ва асосан мутахассисдан ўта эҳтиёткорлик ва масъулиятни талаб этади. Терговчи рақамли далиллар билан ишлашнинг ҳуқуқий, услубий ва ахлоқий талабларини билмасдан туриб, уларнинг мақбуллигини таъминлаши мумкин эмас. Шунга кўра, соҳага оид назарий билимларни шакллантиришда муайян криминалистик билимларга эҳтиёж сезилади[2]. Ҳодиса жойини кўздан кечиришда ёки нарса ва буюмларни кўздан кечиришда нафақат мутахассиснинг махсус билимларга эга

бўлиши балки суриштирувчи-терговчининг ҳам ахборот технологиялари билан ишлашда муайян билимларга эга бўлишлиги муҳим ҳисобланади.

Терговга қадар текширувни амалга оширувчи органнинг мансабдор шахси, суриштирувчи, терговчи ва суд ахборот технологиялари соҳасидаги мутахассис ёки эксперт иштирокида электрон-техник қурилмани ва бошқа электрон маълумотларни ташувчи воситаларни аниқланган жойида электрон ахборотни сақлаш ва олишнинг самарали воситаларидан фойдаланган ҳолда кўздан кечириш лозим бўлади [3].

Ўз ўрнида аниқланган электрон-техник қурилма ёки бошқа турдаги электрон маълумотлар ташувчиси унинг қисмини ташкил этса ёки бир қисми бўлса, электрон маълумотларни қидириб топиш учун терговга қадар текширувни амалга оширувчи органнинг мансабдор шахси, суриштирувчи, терговчи ва суд ахборот технологиялари соҳасидаги мутахассис ёки эксперт иштирокида масофадан туриб компьютер тармоғини кўздан кечириши мумкин ва бу борада юқорида айтиб ўтилганидек махсус билимлар талаб этилади [4]. Агар икки ва ундан ортиқ компьютер тармоқларида қидирилаётган электрон маълумотларнинг бир қисми бўлиши борасида асослар мавжуд бўлса, масофадан туриб кўздан кечириш амалга оширилиши мумкин бўлади [5].

Терговга қадар текширув жараёнидан бошлаб суриштирув ва тергов жараёнларида мобил алоқа воситаси, компьютер техникаси ёки уларнинг қўшимча воситалари ёхуд алоҳида ўзида маълумотларни ташувчи (сақловчи) воситаларни аниқлаш, олиш ва қайд этиш масаласининг кўлами кенг бўлиб, ҳар бири бўйича илмий тадқиқот ишларини олиб бориш ва аниқ ва тўлиқ шаклланган методикани ишлаб чиқиш рақамли экспертизани ўтказиш ва унга объектларни тақдим босқичлари учун аниқ бир манбанинг шакллантирилишига бўлган зарурат кундан-кунга ортиб бораётганлигини кўриш мумкин.

Шундай бўлишига қарамай, бугунги рақамли экспертиза амалиётининг тажрибаларидан келиб чиқиб, ишга илмий ёндошган ҳолда ҳодиса жойини кўздан кечиришда аниқланган компьютер техникаси воситаларини экспертиза учун олиш ва ўрамга олиш жараёнида баённомага қайд этилиши лозим бўлган қуйидаги маълумотлар кетма-кетлигини тергов амалиёти учун тавсия этишни лозим топдик: Текшириш тўғрисидаги баённомада қуйидаги фактлар акс эттирилиши керак:

– объектнинг номи, тури ва мақсади;

– объектнинг жойлашиш ҳолати (қайси хонада, хонанинг қайси нуқтасида);

– объектнинг русуми (махсус белгилари), қўшимча воситаларининг мавжудлиги ва нималардан иборатлиги;

– объектга уланган интернет кабеллари ёки хонадаги симсиз Интернет мосламаларининг мавжудлиги ва жойлашуви, номи, аппарат кўриниши, ранги;

– воқеа содир бўлган жойни ўраб турган бинолар, майдонлар, маъмурий ёки турар жой бинолари, унга яқинлашиш ва уларга бўлган масофа;

– Йўлларнинг, тўхташ жойларининг (бекат, станция ва бошқалар)

жойлашиши;

– қудуқларни, концентраторларни, муҳандислик ва техник коммуникациялар каналларини топиш;

– ахборотни қабул қилишнинг АКТ воситаларидан фойдаланиш билан боғлиқ бўлган ернинг хусусиятлари, тузилиш шакли, тўсиқлар, эшиклар, деразалар мавжудлиги;

– объектни муҳофаза қилиш ҳолати ва жойлашуви, маълумотларнинг тарқалишидан сигнализация воситаларининг мавжудлиги - ёритиш, металл панжаралар, хавфсизлик постлари, қулфлар ва қулфлаш механизмлари, экранлар, ерга улаш воситаси, ёнғин ва хавфсизлик сигнализацияси, ушбу ҳудудга одамларнинг кириш учун назорат пунктлари ва пардалар, жалюзилар, валиклар, махсус кўзойнаклар ва плёнкаларни ҳисобга олиш;

– ахборотни қабул қилишнинг компьютер ва техник воситаларида, хавфсизлик мосламаларида, клавиатураларда, тугмачаларда ва калитларга, симлар ва улагичларда, алмаштириш мосламаларида, розеткаларда ва вилкаларда бармоқ излари, бу жиҳозлардан маълумотларни қабул қилиш ва қабул қилиш воситаларини ёқиш учун мўлжалланганлиги;

– олинган объект ва унинг қўшимча воситаларини ўрамга олишда ишлатилган техник воситалар ва ўрамга олиш усули ва бошқалар.

Мутахассис ўзининг барча техник ҳаракатларини фото ва видео ёзувлар ёрдамида компьютерда ва техник воситаларда қайд этиши, терговчи айни пайтда жиноий-ҳуқуқ қонунчиликда кўрсатилган кўздан кечириш тергов ҳаракатининг процессуал тартибларини тўлиқ бажариши шарт.

Фойдаланилган адабиётлар:

1. Б.Х. Хамидов. Кибержиноятларни тергов қилишда эксперт кўрсатувларини текшириш ва баҳолаш. International conference science and education/uluslararasi konferans bilim ve eğitim. 2021. http://doi.org/10.37057/T_1 (155-158).

2. Криминалистика дарслик Закурлаев.А.К.нинг умумий таҳрири остида, Б.Хамидов 1- жилд IMPRESS MEDIA /2023/-408-413б.

3. Goodstein, D. Reference Manual on Scientific Evidence, 3rd ed., National Academies Press, 2011, ch. The Admissibility of Expert Testimony, pp. 37–54.

4. Астанов И.Р. Мутахассиснинг жиноят процессуал фаолияти: муаммо ва таҳлил // Ўзбекистон Республикаси Бош прокуратурасининг Олий ўқув курслари Ахборотномаси. – Тошкент, 2015. – №4 (24). – Б. 38-41. (12.00.00; №11).

5. Melanie Klinkner. Forensic science expertise for international criminal proceedings: an old problem, a new context and a pragmatic resolution // The international journal of evidence & proof. (2009) №13. – P. 102–103.

KIBERJINOYATCHILIK PROFILAKTIKASI

A.S.Vaxidov

IIV Malaka oshirish instituti Kasbiy tayyorgarlik fakulteti Maxsus fanlar sikli boshlig‘i

Annotasiya. Kiberjinoyatlarning oldini olish, aniqlash va tergov qilish. Mazkur jinoyatlarga qarshi kurashish va oldini olishda mavjud muammolar, shuningdek, Kiberjinoyatchilikka qarshi kurashda qo‘llaniladigan profilaktik usullari. Bu turdagi jinoyatlarni oldini olishga qaratilgan chora-tadbirlar.

Kalit so‘zlar: Kiberjinoyat, profilaktika, profilaktik chora-tadbirlar, hamkorlik yo‘nalishlari, kibirjinoyatlarni kelib chiqish sabablar va imkon bergan shart-sharoitlar.

Профилактика киберпреступности

Аннотация. Предотвращение, выявление и расследование киберпреступлений. Существующие проблемы борьбы и предупреждения указанных преступлений, а также методы профилактики, применяемые в борьбе с киберпреступностью. Меры, направленные на предупреждение данного вида преступлений.

Ключевые слова: Киберпреступность, профилактика, превентивные меры, направления сотрудничества, причины возникновения и условия киберпреступлений.

Prevention of cybercrime

Abstract. Prevention, detection and investigation of cybercrimes. The existing problems of combating and preventing these crimes, as well as prevention methods used in the fight against cybercrime. Measures aimed at preventing this type of crime.

Key words: Cybercrime, prevention, preventive measures, areas of cooperation, causes and conditions of cybercrime.

Xalqaro jinoyatchilikning eng xavfli turlaridan biri bu kiberjinoyatlardir. Kiberjinoyatlarning oldini olish, aniqlash va tergov qilish jarayoni murakkab bo‘lib xususan, bu qilmishni sodir qiluvchi jinoyatchining voqea joyidan uzoqligi va ijtimoiy xavfli oqibatlar kattaligi, shuningdek, ushbu turdagi jinoyatlarni tergov qilishda yagona yondashuvning yo‘qligi va turli mamlakatlar hududlarida hamda milliy darajada o‘zaro ta'sir o‘tkazish tartibi xar-xil ishlab chiqilishi tufayli juda qiyin. O‘zbekiston Respublikasining milliy qonunchiligida maxfiylik va maxfiy ma'lumotlarni himoya qilish maqsadida kiberjinoyatchilikka qarshi kurashishning samarali shakl va usullari izlanmoqda.

So‘nggi paytlarda kiberjinoyatchilikka qarshi kurashish muammosi axborot-kommunikasiya muhitida, shuningdek, kompyuter texnikasidan foydalangan holda qayd etilgan jinoyatlar sonining keskin ortib borayotganini hisobga olgan holda ayniqsa dolzarb bo‘lib qoldi. Axborot texnologiyalarining jadal rivojlanishi, turli xil elektron qurilmalardan foydalanish va Internetga kirish nafaqat mulkni, balki shaxsiy ma'lumotlarni ham zaiflashtirdi.

Shuni ta'kidlash kerakki, hozirgi vaqtda tahlil qilinayotgan muammoning etarlicha murakkabligiga, uning texnik bilimlar bilan bog‘liqligiga qaramay,

mutaxassislar uni oʻrganish va kiberjinoyatchilikka qarshi kurashishning maqbul usullarini topishga qaratilgan koʻp harakatlarni amalga oshirmoqdalar. Axborot-kommunikasiya muhitida sodir etilgan jinoyatlarning oldini olish diqqat markazida boʻlib kelmoqda.

Kiberjinoyatchilikka qarshi kurashda qoʻllaniladigan usullari oldini olinayotgan jinoyat turiga bogʻliq: xakerlik, "burish", tuhmat qilish, spam yuborish, "fishing", kiberhujum, kiber terrorizm va boshqalar. Internet xavfsizligiga faqat turli darajalarda (umumiy, maxsus, yakka tartibda va viktemalogik) qoʻllaniladigan profilaktika choralari orqali erishish mumkin. Kiberjinoyatchilikka qarshi kurash usullarining oʻziga xos xususiyatlaridan kelib chiqqan holda, huquqni muhofaza qilish sohasidagi hamkorlik bu jarayonda ham milliy va xalqaro darajada muhim rol oʻynaydi.

Kiberjinoyatchilikka qarshi kurashish usullari juda aniq va harakat usuliga qarab belgilanadi. Bu axborot va kompyuter tizimlariga toʻgʻridan-toʻgʻri yoki bilvosita kirish orqali ma'lumotlarni yoʻq qilish, blokirovka qilish, nusxalash, oʻzgartirish va ulardan foydalanish boʻlishi mumkin. Profilaktika choralari kompyuter tizimlari orqali olingan ma'lumotlardan foydalanish va olish usullariga, shuningdek jinoyat sabablariga (xudbin impuls), zararli dasturlarning tarqalishiga, bepul dasturiy ta'minotni olish va ulardan foydalanishga, pul oʻgʻirlash, qasos, tijorat josusligi, terroristga yordam berish va boshqalarga qarab bu faoliyatni sodir etish usullariga qarab farq qilishi mumkin.

Kiberjinoyatlarni oldini olish, aniqlash va tergov qilishning murakkabligi quyidagilar bilan belgilanadi:

1) jinoyat sodir etilgan joy va ijtimoiy xavfli oqibatlarni keltirib chiqqan joy bir-biridan uzoqda va turli mamlakatlar hududida joylashgan boʻlishi mumkin;

2) huquqni muhofaza qiluvchi organlar uzoqda boʻlganida jinoyat ishiga tegishli ma'lumotlarning yuqori tezlikda almashinuvi yoki yoʻq boʻlishida.

Qarama-qarshilikning murakkabligi shundaki kiberjinoyatchilikni sodir etgan jinoyatchining shaxsiga, jabrlanuvchi xususiyatlariga, jinoyatni ochish uchun olib borilgan faol tergov choralariga, shuningdek ushbu choralar natijalarini qonuniylashtirishga bogʻliq.

Raqamli va mikroprosessorli qurilmalarni sotib oladigan, aholining huquqiy madaniyatini oshiradigan, shaxsiy ma'lumotlarni oʻz ichiga olgan resurslarga ega boʻlgan xodimlarni yollash, tekshirish va asbobsozlik standartlarini ishlab chiqadigan odamlar bilan tushuntirish suhbati oʻtkazish juda muhimdir, shuningdek, kompyuter tizimlari bilan ishlaydigan shaxslar tomonidan axborot xavfsizligi proseduralari bilan birga rejali va rejadan tashqari tekshiruvlarni oʻtkazish. Shaxsiy ma'lumotlarni himoya qilish, uzatish va yigʻish bilan bogʻliq qonun hujjatlariga muvofiqligini tekshirishni majburiyligini ta'minlash kerak.

Kiberjinoyatlarni sodir etishga imkon beradigan muhim qoidabuzarliklar soniga quyidagilar kiradi:

1) xodimlarning kompyuter ma'lumotlariga ruxsatsiz kirishi;

2) flesh-disklaridan foydalanadigan xodimlar;

3) shaxsiy ma'lumotlarni oʻz ichiga olgan kompyuterlar ustidan nazoratning yoʻqligi;

4) xavf himoyalanmagan va mos antivirus dasturidan foydalanadigan kompyuterlardan foydalanadigan tashkilotlar tomonidan yuzaga keladi;

5) parolni himoya qilish tizimining ish stansiyasiga va uning foydalanuvchi identifikasiyasini ta'minlamaydigan dasturiy ta'minotiga ruxsatsiz kirishdan nomukammalligi;

6) ishda saqlangan parollar ma'lumotlar bazalaridan foydalanish;

7) maxfiylik tartibini majburiy tekshirishning yo‘qligi;

8) xodimlar kompyuter yoki shaxsiy ma'lumotlar, tijorat sirlari yoki boshqa maxfiy ma'lumotlar bilan ishlashda aniqlagan ma'lumotlarni oshkor qilmaslik to‘g‘risida shartnomalar yoki kvitansiyalarning yo‘qligi;

9) shaxsiy ma'lumotlarga, biznes sirlari yoki tijorat maxfiyligini o‘z ichiga olgan ma'lumotlarga yoki boshqa maxfiy ma'lumotlarga ega bo‘lgan barcha xodimlarga ko‘rsatma berilishi kerak, bunda ularning bunday ma'lumotlar bilan ishlash tartibiga rioya qilmaslik uchun javobgarligi tushuntiriladi.

Kiberjinoyatchilikka qarshi kurashish bo‘yicha kriminalistik choralar quyidagilar:

1) tergovda so‘nggi ilmiy yutuqlardan foydalanish;

2) dalillar nazariyasini takomillashtirish, bu nafaqat ashyoviy dalillar va hujjatlashtirilgan ma'lumotlarni, balki virtual va elektron ma'lumotlarni ham ishonchli deb tan olishga imkon beradi;

3) rivojlanish kiberjinoyatlarni sodir etgan shaxslarni aniqlashga imkon beradigan yagona ma'lumotlar bazalari. Virtual va elektron ma'lumotlarga asosiy da'vo shundaki, uning ishonchliligini ta'minlash mumkin emas.

Jinoyatlarni ochish va tergov qilish jarayonida ilmiy yutuqlardan foydalangan holda tergov qilish va ulardan foydalanishning yagona amaliyoti jinoyat sodir etgan shaxsning shaxsini aniqlashga va uni jinoyat sodir etganlikda ayblashga imkon beradi, bu esa o‘z navbatida jazoning muqarrarligi prinsipining bajarilishiga imkon beradi. Jazoning muqarrarligi jinoyatlar sonining kamayishini ham, shaxsning huquqlari va qonuniy manfaatlari bo‘lgan davlatning eng yuqori qadriyatlaridan birini himoya qilishni ham ta'minlashi kerak.

Yuqoridagilarga asoslanib, kiberjinoyatchilikka qarshi kurashning uch asosiy yo‘nalishi mavjud: kriminologik (kiberjinoyatchilikning oldini olish), kriminalistik (jinoyatlarni vaqtincha aniqlash va tergov qilish), jinoyat-huquqi (jinoyatchilarning javobgarligi va jazosining muqarrarligini ta'minlash). Shuningdek, qonunchilik va huquqni muhofaza qilish faoliyatiga e'tibor qaratish va davlat ichida ko‘p bosqichli institusional kiberxavfsizlik tizimini qurishni boshlash kerak.

Kiberxavfsizlik tizimi turli komponentlarni o‘z ichiga olishi kerak, jumladan, aholining raqamli savodxonligi darajasini oshirish, shaxsiy ma'lumotlarni himoya qilishning yakka tartibdagi usullarini ishlab chiqishda yordam berish, shuningdek, kiber tahdidlarga qarshi turish va oldini olish mexanizmlarini joriy etish.

Kiberjinoyatchilikka qarshi kurashning yagona tizimi quyidagi yondashuvlarga asoslanishi kerak:

- kiberxavfsizlik strategiyasini ishlab chiqish;

- kiberjinoyatchilikka qarshi kurashda hamkorlik qiluvchi davlat organlari o‘rtasida qonunchiligining tegishli qoidalarini uyg‘unlashtirish;

- kiberjinoyatchilikka qarshi kurash choralarini nazarda tutuvchi davlatlararo shartnomalar tuzish;

- xalqaro hamkorlikni faollashtirish, yangi texnologik tahdidlarni hisobga olgan holda milliy qonunchilikni takomillashtirish;

- kiberjinoyatchilikka qarshi kurashish uchun zamonaviy moddiy-texnik va kadrlar bazasini shakllantirish;

- texnik va moliyaviy aholining savodxonligi;

- kiberjinoyatchilikka qarshi kurashning barcha ishtirokchilarining huquqni muhofaza qilish organlaridan tortib ilmiy-tadqiqot va ilmiy muassasalargacha bo‘lgan faoliyatini muvofiqlashtirish.

Shunday qilib, kiberjinoyatchilikka qarshi kurashish milliy emas balki xalqaro xarakterdagi dolzarb muammo degan xulosaga kelishimizga imkon beradi. Kiberjinoyatchilikka qarshi kurashish masalalarini tartibga soluvchi etarli miqdordagi normativ-huquqiy hujjatlar mavjudligiga qaramay, hozirda huquqni muhofaza qilish faoliyati samaradorligi haqida gapirish mumkin emas.

Kiberjinoyatchilarga qarshi kurashish, vakolatli axborot siyosatini olib borish, aholini huquqiy tarbiyalash bo‘yicha ish olib borish, kiberjinoyatchilarning javobgarligi va jazosi muqarrarligini ta'minlash uchun zamonaviy moddiy-texnik va kadrlar bazasini shakllantirishga e'tibor qaratish lozim.

Foydalanilgan adabiyotlar:

1. Kompyuter axborot Jinoyat Konvensiya ETS №. 185 (Budapesht, 2001 y 23 noyabr/ Garant: [sayt]. – URL https://base.garant.ru/4089723/;
2. O‘zbekiston Respublikasining 2014-yil 14-maydagi “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi O‘RQ-371-son qonun;
3. O‘zbekiston Respublikasining 1994-yil 22-sentyabrdagi Ma'muriy javobgarlik to‘g‘risidagi kodeksi;
4. O‘zbekiston Respublikasining 1994-yil 22-sentyabrdagi Jinoyat kodeksi.

XUSUSIY TADBIRKORLIKNING XAVFSIZLIGINI TA’MINLASH BO‘YICHA HUQUQNI MUHOFAZA QILISH ORGANLARI ISHINI RAQAMLASHTIRISH MASALALARI

X.X.Baxramov

O‘zbekiston Respubikasi IIV Malaka oshirish instituti Yuridik fanlar kafedrasi dotsenti

Annotatsiya. Raqamli texnologiyalarning jadal rivojlanishi va kiberjinoyatlar tahdidining kuchayishi munosabati bilan ma’lumotlarni himoya qilish va kiberxavfsizlikni ta’minlash huquqni muhofaza qiluvchi organlar uchun muhim ahamiyat kasb etmoqda. Ushbu maqolada ma’lumotlar xavfsizligini ta’minlashga qaratilgan zamonaviy texnologiyalarni joriy etish, shuningdek, kibertahdidlarga qarshi kurashda qo‘llaniladigan usullar va strategiyalar ko‘rib chiqilgan. Xodimlarni o‘qitish, muntazam tekshiruv va test sinovlarini o‘tkazib borish, tahdid(hodisa)larga qarshi

rejalar ishlab chiqish muhimligiga e’tibor qaratilgan. Bundan tashqari, boshqa tashkilotlar bilan hamkorlik qilish va qonunchilikka rioya qilish zarurati ta’kidlangan.

Kalit so‘zlar: axborot texnologiyalari, ma’lumotlarni himoya qilish, ma’lumotlarni shifrlash, video kuzatuv va intellektual tizimlar, kiberxavfsizlik, kiberxavfsizlik tahdidlari, xavfsizlik auditi, ma’lumotlarni himoya qilish qonunchiligi, huquqni muhofaza qilish organlari, xodimlarni o‘qitish.

Аннотация. В условиях быстрого развития цифровых технологий и растущей угрозы киберпреступности защита данных и кибербезопасность становятся критически важными для правоохранительных органов. Данная статья рассматривает внедрение современных технологий, направленных на обеспечение безопасности данных, а также методы и стратегии, используемые для борьбы с киберугрозами. Особое внимание уделяется важности обучения сотрудников, проведению регулярных проверок и тестирований, а также разработке планов реагирования на инциденты. Кроме того, рассматривается необходимость сотрудничества с другими организациями и соблюдения законодательных норм.

Ключевые слова: информационные технологии, защита данных, шифрование данных, видеонаблюдение и интеллектуальные системы, кибербезопасность, угрозы кибербезопасности, аудит безопасности, законодательство о защите данных, правоохранительные органы, обучение сотрудников.

Annotation. With the rapid advancement of digital technology and the growing threat of cybercrime, data protection and cybersecurity are becoming critical for law enforcement agencies. This article examines the implementation of modern technologies aimed at ensuring data security, as well as the methods and strategies used to combat cyber threats. Emphasis is placed on the importance of employee training, conducting regular audits and testing, and developing incident response plans. In addition, the need for cooperation with other organizations and compliance with legal regulations is considered.

Keywords: information technology, data protection, data encryption, video surveillance and intelligent systems, cybersecurity, cybersecurity threats, security audit, data protection legislation, law enforcement, employee training.

Texnologiya aql bovar qilmaydigan tezlikda rivojlanayotgan zamonaviy dunyoda raqamlashtirish hayotning barcha jabhalarining, jumladan, huquqni muhofaza qiluvchi organlarning ham ajralmas qismiga aylanib bormoqda. Raqamli texnologiyalar xususiy biznes xavfsizligini ta’minlash, jinoyatchilikka qarshi kurashish, huquqbuzarliklarning oldini olish va tadbirkorlar manfaatlarini himoya qilishda yangi imkoniyatlar yaratadi.

Ichki ishlar organlari faoliyatini raqamlashtirishning muhim jihatlaridan biri zamonaviy texnologiyalarni joriy etishdan iborat. Videokuzatuv tizimlari, katta ma’lumotlar tahlili, biometrik texnologiyalar va sun’iy intellekt huquqni muhofaza qilish organlariga jinoyatlarni yanada samaraliroq aniqlash va oldini olish imkonini

beradi. Misol uchun, jamoat joylarida va biznes binolarida videokuzatuv imkoniyatlari natijasida hodisalarga tezkor ta’sir qilish jiddiy xaf-xatarlarni oldini olish bartaraf etishda va keyingi tergov harakatlari uchun dalillar to'plashga yordam beradi.

Huquqni muhofaza qilish organlariga zamonaviy texnologiyalarning joriy etilishi ularning samaradorligini oshirish va tez o‘zgaruvchan dunyoga moslashish yo‘lidagi muhim qadamdir. Bu jarayon ish sifatini oshirish, jinoyatchilikni kamaytirish va fuqarolar xavfsizligini oshirishga yordam beradigan turli vositalar va tizimlardan foydalanishni nazarda tutadi. Keling, qanday texnologiyalar joriy etilayotgani va joriy etilishi zarur bo‘lgan chora-tadbirlarni hamda ularni huquqni muhofaza qilish organlari faoliyatiga qanday samarali ta'sir ko'rsatishini batafsil ko'rib chiqaylik.

1) Video kuzatuv va intellektual tizimlar. Eng ko'zga tashlanadigan texnologiyalardan biri bu video kuzatuv tizimi. O'rnatilgan kameralar nafaqat voqealarni yozib olish, balki mashinani o'rganish algoritmlaridan foydalanadigan aqlli tizimlarga ham ulanishi mumkin. Bunday tizimlar shubhali odamlar yoki vaziyatlarni avtomatik ravishda tanib, huquqni muhofaza qilish organlarini mumkin bo'lgan huquqbuzarliklar haqida ogohlantiradi. Bu javob tezligini sezilarli darajada oshiradi va jinoyatlarning oldini olishga yordam beradi, shuningdek, dalillarni ta'minlashning yordamchi usuli hisoblanadi.

2) Katta ma'lumotlarni tahlil qilish. Katta ma'lumotlar tahlili huquqni muhofaza qilish organlariga jinoyat va huquqbuzarlik haqida katta hajmdagi ma'lumotlarni qayta ishlash imkonini beradi. Ma'lumotlarni tahlil qilish tizimlari jinoiy faoliyatning naqshlari va tendentsiyalarini aniqlay oladi, bu potentsial jinoyatlarni bashorat qilishga va resurslarni eng zaif hududlarga yo'naltirishga yordam beradi. u huquqni muhofaza qilish organlariga tahdidlarga yanada aniqroq javob berish va operatsion strategiyani takomillashtirish imkonini beradi.

3) Biometrik texnologiyalar. Yuzni aniqlash, barmoq izini aniqlash va ovozni aniqlash kabi biometrik tizimlar xavfsizlik darajasini sezilarli darajada oshiradi. Ular gumondorlarni tezda aniqlash va huquqbuzarliklarni qayd etish jarayonini soddalashtirish imkonini beradi. Huquq-tartibot idoralari biometrik ma’lumotlar yordamida gumonlanuvchilar haqidagi ma’lumotlarni tezkorlik bilan qo‘lga kiritishi va ularni boshqa jinoyatlarga bog‘lashi mumkin, bu esa tergovni sezilarli darajada tezlashtiradi.

4) Mobil ilovalar va onlayn platformalar. Fuqarolar bilan muloqot qilish uchun mobil ilovalar va onlayn platformalarning joriy etilishi ham huquqni muhofaza qiluvchi organlar faoliyatini raqamlashtirishning muhim qismiga aylandi. Bunday ilovalar fuqarolarga jinoyatlar haqida xabar berish, ularning ishlarining holati haqida ma’lumot olish va yordam so‘rash imkonini beradi. Bu nafaqat fuqarolar va huquqni muhofaza qiluvchi idoralar o‘rtasidagi o‘zaro munosabatlarni soddalashtiradi, balki huquqni muhofaza qiluvchi organlarga ishonch darajasini oshiradi.

5) Kiberxavfsizlik va ma'lumotlarni himoya qilish. Raqamli texnologiyalar kuchayib borayotgani sari kiberjinoyat tahdidlari ham ortadi. Huquq-tartibot idoralari ma’lumotlarni himoya qilishning zamonaviy texnologiyalarini joriy etish orqali kiberxavfsizlikka alohida e’tibor qaratishi lozim. Bu kiberjinoyatlarga qarshi kurash bo‘yicha ixtisoslashtirilgan bo‘linmalarni yaratish, shuningdek, xodimlarni axborotni himoya qilish va kiberhujumlarga javob qaytarish bo‘yicha o‘qitishni o‘z ichiga oladi.

6) Avtonom tizimlar va dronlar. Hududlarni patrul qilish va kuzatish uchun avtonom tizimlar va dronlardan tobora ko'proq foydalanilmoqda. Ushbu qurilmalar borish qiyin bo'lgan joylarda tekshiruvlar o'tkazishi, shuningdek, real vaqt rejimida ma'lumotlarni to'plashi mumkin, bu esa huquqni muhofaza qilish organlariga vaziyatlarga tezda javob berishga imkon beradi. Dronlardan dalillar to‘plash va ommaviy hodisalarni kuzatish, xavfsizlikni oshirish uchun ham foydalanish mumkin.

Yuqoridagilardan kelib chiqqan holda shuni ta’kidlash mumkinki, huquqni muhofaza qiluvchi organlar, xususan, ichki ishlar organlari faoliyatiga zamonaviy texnologiyalar joriy etilayotgani ularning samaradorligi va xavfsizligini oshirishda muhim ahamiyat kasb etmoqda.

Videokuzatuv, katta ma’lumotlar tahlili, biometrik texnologiyalar va boshqa innovatsiyalardan foydalanish huquqni muhofaza qiluvchi organlarga tahdidlarga tezkor javob berish, jinoyatlarning oldini olish va fuqarolarni himoya qilish imkonini beradi. Zamonaviy texnologiyalar xavfsizlik sohasida yangi ufqlarni ochadi, ularning yanada rivojlanishi va huquqni muhofaza qilish organlari faoliyatiga integratsiyalashuvi jamiyat xavfsizligini ta’minlashning asosiga aylanadi. Samarali kommunikatsiyalar, ma'lumotlarni himoya qilish va kiberxavfsizlik kabi.

- *Samarali kommunikatsiyalar (to‘g‘ri tashkil etilgan aloqa).* Raqamlashtirish, shuningdek, huquqni muhofaza qilish organlari va biznes o'rtasidagi aloqani yaxshilashga yordam beradi. Axborot almashish platformalari huquqbuzarliklar va tahdidlar to‘g‘risidagi ma’lumotlarni tez va samarali tarzda uzatish, shuningdek, korxonalardan fikr-mulohazalarni olish imkonini beradi. Bu biznes so'rovlariga tezroq javob berishga va umumiy xavfsizlik darajasini yaxshilashga yordam beradi.

- *Ma'lumotlarni himoya qilish va kiberxavfsizlik.* Raqamli texnologiyalar o'sib borishi bilan kiberxavfsizlik tahdidlari soni ortib bormoqda. Huquqni muhofaza qilish organlari xususiy kompaniya ma'lumotlarini kiberhujumlardan himoya qilishda muhim rol o'ynaydi. Kiberjinoyatlarga qarshi kurashish bo‘yicha ixtisoslashtirilgan bo‘linmalarning tashkil etilishi, xodimlarni o‘qitish va biznes vakillari bilan hamkorlikda kiberxavfsizlik darajasini oshirish bu boradagi muhim qadamlardandir. Raqamlashtirish davrida ma'lumotlar xavfsizligi va kiber tahdidlar huquqni muhofaza qilish organlarining muhim jihatlariga aylandi. Yangi texnologiyalarni joriy etish samaradorlikni oshirish uchun ko'plab imkoniyatlarni beradi, lekin yangi xavflarni ham keltirib chiqaradi.

Keling, huquqni muhofaza qilish organlari ma'lumotlarni qanday himoya qilishini va kiberxavfsizlikni ta'minlashini ko'rib chiqaylik.

Kiberxavfsizlikka tahdidlar. Huquqni muhofaza qilish organlari duch keladigan kibertahdidlar turlicha bo'lishi mumkin:

Hacker hujumlari: ma'lumotlarni o'g'irlash, o'zgartirish yoki yo'q qilish maqsadida tizimlarga ruxsatsiz kirishga urinishlar.

Fishing: maxfiy ma'lumotlarni olish uchun soxta xabarlar yoki veb-saytlardan foydalanish. Zararli dasturlar: Viruslar va troyan otlari kabi tizimlar yoki ma'lumotlarga zarar etkazishi mumkin bo'lgan dasturlar [1].

Ma'lumotlar xavfsizligini ta'minlash uchun huquqni muhofaza qilish organlari bir qancha strategiyalarni qo'llashlari kerak:

A) Ma'lumotlarni shifrlash: uzatish va saqlash vaqtida axborotni himoya qilish uchun shifrlash algoritmlaridan foydalanish. Bu sizib chiqish yoki buzish holatlarida ma'lumotlarga kirishni oldini olishga yordam beradi.

B) Dasturiy ta'minotni muntazam yangilash: tajovuzkorlar tomonidan ishlatilishi mumkin bo'lgan zaifliklarni yopish uchun barcha tizimlar va dasturlarni yangilab turish.

C) Ko'p faktorli autentifikatsiya: tizimlar va ma'lumotlarga kirishda bir nechta darajadagi tekshirishdan foydalanish. Bu xakerlik qilishni qiyinlashtiradi va vaqt talab etadi. Bizning fikrimizcha, xavfsizlikni ta'minlashga qaratilgan zarur chora-tadbirlar quyidagilardan iborat:

1) Ichki ishlar organlari xodimlarini tayyorlash va malakasini oshirish - kiberxavfsizlik masalalari ma'lumotlarni himoya qilishning ajralmas qismidir. Huquq-tartibot idoralari hamkorlikda xodimlarga kibertahdidlarni aniqlash, tanib olish, hodisalarga tezkor javob berish va belgilangan qoida va yo‘riqnomalarga rioya qilishni o‘rgatish maqsadida muntazam treninglar o‘tkazilishi muhim ahamiyat kasb etadi. O'zingizni va ma'lumotlaringizni qanday himoya qilishni bilish hujumlar xavfini sezilarli darajada kamaytiradi.

2) Kiberxavfsizlik hodisalarini kuzatish va ularga javob berish. Huquqni muhofaza qilish organlari o'zlarining axborot tizimlaridagi faoliyatni kuzatish imkonini beruvchi monitoring tizimlarini joriy qilmoqdalar. Bunga quyidagilar kiradi:

-log tahlili: shubhali faoliyatni aniqlash uchun kirish jurnallarini kuzatish va tahlil qilish;

-hodisa-javob: kiberhujumlarga tezda javob bera oladigan va zararni minimallashtiradigan ixtisoslashgan guruhlarning mavjudligi;

-boshqa tegishli tashkilotlar bilan hamkorlik va o'zaro hamkorlik, chunki kibertahdidlar ko'pincha chegaraga ega emas, shuning uchun boshqa davlat organlari, xususiy kompaniyalar va xalqaro tashkilotlar bilan hamkorlik kiberxavfsizlikning muhim jihatiga aylanadi. Yangi tahdidlar va mudofaa usullari haqida ma'lumot almashish umumiy xavfsizlikni yaxshilashi mumkin.

3) Qoidalar va standartlarga muvofiqligi. Huquqni muhofaza qilish organlari ma'lumotlarni himoya qilish sohasida amaldagi qonunlar va xalqaro standartlarga rioya qilishlari shart. Bunga Evropada ma'lumotlarni himoya qilish bo'yicha umumiy reglament (GDPR) yoki boshqa mamlakatlardagi shunga o'xshash qonunlar kabi shaxsiy ma'lumotlarni qayta ishlash qoidalariga rioya qilish kiradi[2];

4) Profilaktik chora-tadbirlar. Raqamlashtirish huquqni muhofaza qilish organlariga profilaktika choralariga e'tibor qaratish imkonini beradi. Jinoiy faoliyat ma'lumotlarini tahlil qilish va ehtimoliy jinoyatlarni modellashtirish tahdidlarni aniqroq bashorat qilish va oldini olish imkonini beradi. Masalan, geografik tahlil yordamida huquq-tartibot idoralari jinoyatchilikning qaynoq nuqtalarini aniqlashi va bu hududlarda profilaktika tadbirlarini tashkil etishi;

5) Biznes vakillari bilan hamkorlik. Xususiy biznes bilan faol hamkorlik qilmasdan turib, huquqni muhofaza qiluvchi organlar faoliyatini samarali raqamlashtirish mumkin emas. Davlat organlari va tadbirkorlar o‘rtasida hamkorlik aloqalarining o‘rnatilishi xavfsizlik bo‘yicha qo‘shma dasturlarni ishlab chiqish, tajriba

va resurslar almashish imkonini beradi. Bu hamkorlik nafaqat xavfsizlikni yaxshilaydi, balki biznes muhitini ham yaxshilaydi.

Yuqoridagilardan kelib chiqqan holda, bizning fikrimizcha, huquqni muhofaza qiluvchi organlarda ma’lumotlar himoyasi va kiberxavfsizlikni ta’minlash kompleks yondashuvni hamda turli strategiya va vositalardan foydalanishni talab qiladi.

Fikrimizcha, huquqni muhofaza qilish organlarida ma'lumotlarni samarali himoya qilish va kiberxavfsizlikni ta'minlash uchun quyidagi tavsiyalarga amal qilish maqsadga muvofiq bo'ladi:

1. Kiberxavfsizlik strategiyalarini ishlab chiqish va amalga oshirish. Keng qamrovli kiberxavfsizlik rejasini yaratish: kiberxavfsizlikning barcha jihatlarini, jumladan, xavflarni boshqarish, hodisalarga tezkor javob berishni qamrab oluvchi strategiyani ishlab chiqish. Shuningdek, strategiyalarni muntazam yangilab turing: Yangi tahdidlar va texnologiyalarga muvofiq strategiyalarni vaqti-vaqti bilan ko'rib chiqing va yangilang.

2. Xodimlarning xabardorligini oshirish, o'qitish va rivojlantirish. Muntazam treninglar: Barcha xodimlar (ayniqsa, yosh xodimlar) uchun kiberxavfsizlik bo'yicha treninglar o'tkazish, shu jumladan fishing, zararli dasturlar va boshqa tahdidlardan himoya qilish usullari haqida ma'lumot. Xavfsizlik madaniyatini shakllantirish: xodimlarni har qanday shubhali faoliyat yoki hodisalarni aniqlash, xabar berish va bostirishga undash.

3. Zamonaviy himoya texnologiyalaridan foydalanish. Ma'lumotlarni shifrlash: maxfiy ma'lumotlarni uzatish paytida ham, saqlash vaqtida ham himoya qilish uchun shifrlashdan foydalanish.

Ko'p faktorli autentifikatsiya: tizimlar va ma'lumotlarga kirish uchun ko'p faktorli autentifikatsiyani amalga oshiring, bu xavfsizlik darajasini oshiradi.

4. Muntazam tekshiruvlar va testlarni o'tkazish. Xavfsizlik auditini o‘tkazish: xavfsizlik tizimlarining zaif va sust tomonlarini aniqlash uchun muntazam ravishda ichki va tashqi auditlarni o'tkazish tavsiya etiladi. Buzib kirish testlarini o‘tkazish: Xavfsizlik darajasini baholash va mumkin bo'lgan zaifliklarni aniqlash uchun buzib kirish testlarini o'tkazib borish.

5. Hodisalarni bartaraf etish rejalarini ishlab chiqish. Javob berish guruhlarini tashkil etish: Ixtisoslashgan guruhlarni shakllantirish (kiberhujumlar va hodisalarga javob berish uchun mas'ul bo'lgan guruhlar. Harakat rejalari: Voqea sodir bo'lganda harakatlar uchun aniq ko'rsatmalar ishlab chiqish, shu jumladan xabar berish va tiklash tartib-qoidalari.

6. Boshqa tashkilotlar bilan hamkorlik va o'zaro hamkorlik. Axborot almashinuvi: yangi tahdidlar va himoyalanish usullari haqida ma’lumot almashish uchun boshqa huquqni muhofaza qiluvchi organlar va xususiy kompaniyalar bilan shartnomalar, hamkorlik memorandumlari va o‘zaro hamkorlik. Xavfsizlik tarmoqlarida tizimli ishtirok etish: eng yaxshi amaliyotlar bo'yicha resurslar va ma'lumotlarga kirish uchun milliy va xalqaro kiberxavfsizlik tashabbuslariga qo'shilish.

7. Qonunchilik va standartlarga rioya qilish. Muvofiqlik: Ma'lumotlarni himoya qilish bo'yicha barcha amaldagi qonunlar va qoidalarga, shu jumladan GDPR standartlari va boshqa mahalliy qoidalarga muvofiqligini ta'minlash. Jarayon hujjatlari:

ma'lumotlarni qayta ishlash va himoya qilish bilan bog'liq barcha jarayonlar va protseduralarning to'liq hujjatlarini yuritish. Kiberxavfsizlik to‘g‘risidagi milliy qonunchilik “Kiberxavfsizlik to‘g‘risida”gi qonun va boshqa qonun hujjatlaridan iborat. Telekommunikatsiya tarmoqlari va aloqa kanallari bo‘yicha tezkor-qidiruv tadbirlari tizimining kiberxavfsizligini ta’minlash alohida qonun hujjatlarida belgilangan tartibda amalga oshiriladi.

Agar O‘zbekiston Respublikasining xalqaro shartnomasida O‘zbekiston Respublikasining kiberxavfsizlik to‘g‘risidagi qonun hujjatlarida nazarda tutilganidan boshqacha qoidalar belgilangan bo‘lsa, xalqaro shartnoma qoidalari qo‘llaniladi [3].

Yuqoridagilardan kelib chiqib, quyidagi xulosalar chiqarish mumkin.

Ma'lumotlarni himoya qilish va kiberxavfsizlik zamonaviy raqamli voqelikda huquqni muhofaza qilish organlari uchun eng muhim vazifalardir. Kibertahdidlar ortib borayotgan bir sharoitda huquqni muhofaza qilish idoralari o'z strategiyalari, texnologiyalari va amaliyotlarini doimiy ravishda takomillashtirib borishlari kerak.

Xodimlarni tayyorlash, malakasini oshirish, zamonaviy texnologiyalarni joriy etish va boshqa tashkilotlar bilan hamkorlik qilish ishonchli ma’lumotlarni himoya qilish tizimini yaratishga yordam beradi, bu esa, o‘z navbatida, butun jamiyat xavfsizligi darajasini oshiradi. Huquqni muhofaza qilish organlarida ma’lumotlar himoyasi va kiberxavfsizlikni ta’minlash murakkab va ko‘p qirrali vazifadir. Yuqoridagi tavsiyalarni qo'llash xavflarni minimallashtirish va xavfsizlik darajasini oshirishga yordam beradigan ishonchli himoya tizimini yaratishga yordam beradi. Kibertahdidlar doimo o'zgarib borayotgan bir sharoitda yangi chaqiriqlarga tayyor bo'lish va kiberxavfsizlik strategiyalarini zamonaviy voqelikka mos ravishda moslashtirish muhim ahamiyatga ega.

Huquqni muhofaza qilish organlari faoliyatini raqamlashtirish xususiy tadbirkorlik subyektlari xavfsizligini ta’minlashda yangi ufqlarni ochmoqda. Zamonaviy texnologiyalarni joriy etish, samarali muloqot, ma’lumotlarni himoya qilish va faol hamkorlik qilish, biznes vakillari bilan o‘zaro hamkorlik – bularning barchasi yanada xavfsiz va barqaror ishbilarmonlik muhitini yaratishga xizmat qilmoqda. Jadal o'zgarib borayotgan dunyoda o'zgarishlarga va yangi texnologiyalarga moslashishga tayyorlik huquqni muhofaza qilish idoralari va xususiy biznes uchun asosiy muvaffaqiyat omillariga aylanmoqda.

Foydalanilgan adabiyotlar ro‘yxati:

[1] Easttom, C. (2021). Cybersecurity: A Beginner's Guide. McGraw-Hill.

[2] European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union.

[3] O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son qonuni 15.04.2022 y., Qonunchilik ma’lumotlari milliy bazasi, 16.04.2022 y., 03/22/764/0313-son.

ОБЩАЯ АРХИТЕКТУРА СИСТЕМ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ

Ашуралиев А.А., Абдишукуров Ш.М., Омонова М.Ш.

Ташкентский государственный технический университет имени Ислама Каримова

Сегодня проводится множество научных исследований, направленных на обработку и анализ больших данных. Создание эффективной архитектуры систем обработки больших данных является ключевым аспектом для достижения успеха в анализе и использовании данных. Использование таких данных широко применяется в производстве, экономике, социальных и других сферах, что также способствует развитию этих технологий. Любая информационная система для хранения и анализа больших данных должна быть основана на определенной аппаратной и программной архитектуре. Архитектура системы, работающей с большими данными, представлена на рисунке 1.

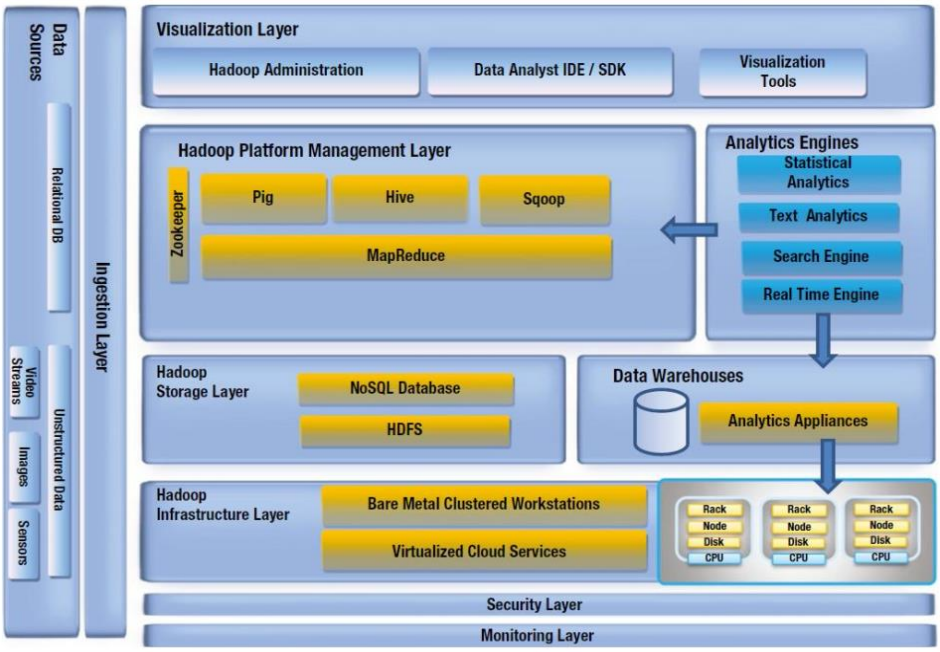


Рис.1. Архитектура системы хранения и анализа больших данных.

Уровень источников данных (Data Sources). Предприятия обычно имеют несколько внутренних и внешних источников данных. Также существуют требования по очистке, проверке и масштабированию данных перед их записью.

Слой загрузки данных (Ingestion Layer). Слой загрузки (рисунок 2) является новым слоем обработки корпоративных данных. Этот слой отвечает за отделение шума от соответствующих данных. Алгоритмы в этом слое должны иметь возможность проверять, очищать, трансформировать, сокращать и агрегировать данные в технический стек больших данных для дальнейшей обработки. Это расширяемая, устойчивая к ошибкам, гибкая и регулирующая программа в архитектуре больших данных. В соответствии с процессом Data Science, ошибки в этом слое могут отменить все последующие операции.

Уровень источников данных. NoSQL, HDFS, идентификация, фильтрация, валидация, уменьшение шума, трансформация, сжатие, интеграция.

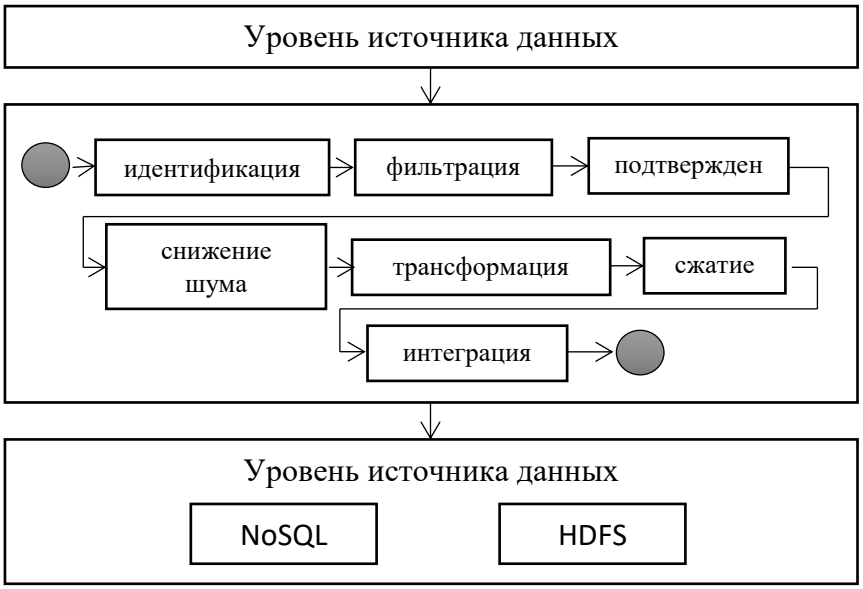


Рис. 2. Роль слоя загрузки данных в архитектуре приложений для хранения и анализа больших данных.

Примеры в архитектуре, приведенные выше, описывают решение общих проблем источников данных с точки зрения воздействия на слой загрузки. Эти решения могут быть выбраны на основе требований к производительности, масштабируемости и доступности.

Общие модели загрузки данных:

1. Multisource Extractor Pattern – подход для эффективного использования различных источников данных.
2. Protocol Converter Pattern – использование брокера протоколов для абстрагирования входящих данных от различных протокольных слоев.
3. Multidestination Pattern – сценарий, в котором слой загрузки должен переносить данные в несколько компонентов хранения, таких как Hadoop, колоночные базы данных или механизмы реального времени.
4. Just-in-Time Transformation Pattern – данные преобразуются только тогда, когда это необходимо для экономии вычислительного времени.
5. Real-Time Streaming Patterns – в условиях, когда бизнес-задачи требуют оперативного анализа входящих данных, необходима загрузка и анализ данных в реальном времени.

Слой безопасности (Security Layer)Так как анализ больших данных стал одной из важнейших задач для организаций, безопасность этих данных также является приоритетом. Хранимые данные и результаты их обработки должны быть защищены в соответствии с требованиями конфиденциальности. Поэтому средства авторизации и аутентификации должны быть планированы с самого начала.

Основные меры безопасности:

1. Шифрование на уровне файлов.
2. Подписка на службы управления ключами и сертификатами.
3. Регистрация и использование распределенных систем для связи между узлами.
4. Механизмы мониторинга аномалий на различных уровнях.
5. Обеспечение безопасности связи между узлами, например, с использованием SSL, TLS и других.

Слой мониторинга (Monitoring Layer).

Системы мониторинга используются для отслеживания состояния распределенных кластеров и сбора информации о операционных системах, аппаратных средствах и прочем. Для выполнения этой задачи машины должны связываться с инструментами мониторинга через высокоуровневые протоколы, такие как XML, а не двоичные форматы. Системы мониторинга также должны предоставлять инструменты для хранения и визуализации данных.

Архитектура систем обработки больших данных включает несколько уровней, таких как сбор, хранение, обработка и анализ данных. Важным аспектом является использование гибридных баз данных (SQL и NoSQL) для обработки как структурированных, так и неструктурированных данных. Безопасность данных обеспечивается многоуровневыми механизмами, включая шифрование и управление доступом. Для эффективного мониторинга и управления рекомендуется использовать современные инструменты, такие как Prometheus и Grafana.

Литература

1. Интегрированная информационно-аналитическая система конструкторско-технологической подготовки производства [Электронный ресурс]. – URL: http://library.ziyonet.uz/ru/book/download/108551 (10.09.2021)
2. Dean, J., & Ghemawat, S. (2008). MapReduce: Simplified Data Processing on Large Clusters. Communications of the ACM, 51(1), 107-113.
3. Marz, N., & Warren, J. (2015). Big Data: Principles and Best Practices of Scalable Real-Time Data Systems. Manning Publications.
4. Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The Rise of "Big Data" on Cloud Computing: Review and Open Research Issues. Information Systems, 47, 98-115.

KIBERJINOYATCHILIKKA QARSHI KURASHISHDA ZAMONAVIY TEXNOLOGIYALAR VA HUQUQIY MEXANIZMLARNING O‘RNI

IIV Akademiyasi Behruzjon Bozorov
IIV TQD Kiberxavfsizlik markazi Shohrux Azizxonov

Zamonaviy dunyoda texnologiyalar hayotning barcha jabhalarini qamrab olmoqda. Shu bilan birga, axborot texnologiyalari rivoji kiberjinoyatchilik xavfini ham oshirmoqda. Kiberjinoyatchilikning murakkabligi va tez o‘zgaruvchanligi unga qarshi

samarali kurash choralarini ishlab chiqishni talab etadi. Mazkur tezisda kiberjinoyatchilikning huquqiy, tashkiliy va texnologik jihatlari tahlil qilinadi.

Kiberjinoyatchilik tushunchasi va uning huquqiy ta'rifi

O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi qonuning 3-moddasida kiberjinoyatchilik tushunchasiga ta’rif berilgan. Unga ko‘ra kiberjinoyatchilik-axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisidir. Xalqaro huquqda ushbu tushuncha keng qamrovli bo‘lib, kiberfiribgarlik, shaxsiy ma'lumotlarni o‘g‘irlash va axborot tizimlariga noqonuniy kirishni o‘z ichiga oladi. Ushbu huquqiy ta'riflar dunyo davlatlarining milliy qonunchiliklarida turlicha bo‘lib, ularni birlashtirish xalqaro hamkorlik uchun muhim ahamiyatga ega.

Kiberjinoyatchilikka qarshi kurashning tashkiliy jihatlari

Bugungi kunda yurtimizda kiberjinoyatchilikka qarshi kurashuvchi vakolatli organlar va ular negizida maxsus bo‘linmalar faoliyat olib bormoqda. Masalan, O‘zbekiston Respublikasi Ichki Ishlar Vazirligi Tezkor-qidiruv Departamenti huzuridagi kiberxavfsizlik markazi, O‘zbekiston Respublikasi Davlat Xavfsizlik Xizmati huzuridagi Kiberxavfsizlik DUK. Ushbu organlar kiberjinoyatlar, shu jumladan, internet orqali amalga oshiriladigan kiberfiribgarliklar, shaxsiy ma'lumotlarni o‘g‘irlash, tizimlarga noqonuniy kirish va boshqa kiberjinoyatlarni aniqlash va oldini olish bilan shug‘ullanib kelmoqda. Biroq, hozirgi vaqtda ushbu bo‘linmalarning moddiy-texnik bazasini kuchaytirish va mutaxassislarni tayyorlash masalalari dolzarb bo‘lib qolmoqda. Chunki hozirgi vaqtda kiberxavfsizlik sohasidagi mutaxassislar yuqori malakaga ega bo‘lishi, zamonaviy texnologiyalarni tushunishi va ularni samarali qo‘llay olishlari zarur. Ushbu sohada tayyorlangan kadrlar orqali kiberxavfsizlikning samaradorligini oshirish, kiberhujumlarni va boshqa kiberjinoyatlar turlarini oldini olish mumkin. Bunday tashkiliy va texnik choralar mamlakatimizning kiberxavfsizlikni ta'minlashdagi yutuqlarini kuchaytiradi va jinoyatlarning oldini olishda samarali vositalarni yaratadi.

Sun’iy intellekt (AI) texnologiyalarining kiberjinoyatchilikka qarshi kurashdagi o‘rni

Sun’iy intellekt (AI) texnologiyalari, ayniqsa, **mashinaviy o‘rganish (machine learning)** va **chuqur o‘rganish (deep learning)** algoritmlari kiberjinoyatlarni aniqlash va oldini olishda muhim vosita hisoblanadi. Ushbu texnologiyalar kiberxavfsizlik sohasida yangi imkoniyatlarni yaratib, kiberjinoyatlar va firibgarliklarni oldindan aniqlash, tarmoq xavfsizligini ta’minlashda samarali yechimlar taqdim etadi.

1. **Mashinaviy o‘rganish va chuqur o‘rganish algoritmlari**

Mashinaviy o‘rganish (ML) algoritmlari tarmoqda yoki tizimlarda yuzaga kelgan harakatlarni real vaqtda tahlil qiladi va g‘ayrioddiy (anonym) xatti-harakatlarni aniqlashga yordam beradi. Mashinaviy o‘rganish modellari avvalgi kiberhujumlar yoki noxush faoliyatlarni tahlil qilib, kelajakdagi shunga o‘xshash xavf-xatarlarni oldindan aniqlash uchun o‘z-o‘zini takomillashtiradi.

Chuqur o‘rganish (deep learning) texnologiyalari esa yanada murakkab tizimlar orqali yanada aniq va samarali tahminlar beradi. Chuqur o‘rganish algoritmlari, ayniqsa, tarmoqdagi xavfsizlikni monitoring qilishda qo‘llaniladi. Misol uchun, ularni kiberhujumlarini aniqlashda, soxta ma’lumotlarni filtrlashda va kiberhujumchilar tomonidan ishlatiladigan yangi texnikalar yoki vositalarni tahlil qilishda foydalanish mumkin.

2. **Misollar:**

Singapur hukumati o‘zining kiberxavfsizlik tizimida sun’iy intellekt va mashinaviy o‘rganishdan faol foydalanadi. Singapurda **Singapur kiberxavfsizlik agentligi** (CSA) tomonidan kiberhujumlarni aniqlash va oldini olish uchun sun’iy intellekt texnologiyalari qo‘llaniladi. Ular kiberxavfsizlik tizimlariga AI asoslangan tizimlarni joriy qilgan bo‘lib, tarmoqdagi barcha harakatlarni tahlil qiladi, ularni normal va abnormal holatlarga ajratib, tarmoqdagi xavflarni tezda aniqlaydi.

Yaponiyada kiberxavfsizlikni ta’minlash uchun sun’iy intellekt asosida ishlaydigan tizimlar ishlab chiqilgan. Masalan, **NTT Communications** kompaniyasi kiberxavfsizlikni boshqarish uchun AI texnologiyalaridan foydalanadi. Ushbu tizimlar kiberhujumlarni aniqlashda va tarmoq faoliyatini monitoring qilishda mashinaviy o‘rganish algoritmlarini qo‘llaydi. Xususiy sektorda AI asosida ishlaydigan tizimlar, masalan, ma’lumotlarni himoya qilish va firibgarlikni aniqlashda ham muvaffaqiyatli ishlamoqda.

Huquqiy mexanizmlar va xalqaro hamkorlik: Budapesht Konvensiyasi

Kiberjinoyatchilikning transchegaraviy xususiyati uni faqat mamlakat chegaralari doirasida hal qilinishini qiyinlashtiradi. Shuning uchun, xalqaro hamkorlik kiberjinoyatchilikka qarshi kurashishda muhim rol o‘ynaydi. **Budapesht Konvensiyasi** 2001-yil 23-noyabrda tuzilgan bo‘lib, kiberjinoyatchilikka qarshi kurashishda asosiy xalqaro huquqiy hujjatlardan biri hisoblanadi. Bugungi kunga qadar ushbu konvensiyaga 70 dan ortiq davlatlar a’zo bo‘lgan, jumladan, AQSh, Yevropa Ittifoqi davlatlari va boshqa ko‘plab davlatlar. Konvensiya kiberjinoyatchilikning oldini olish, uning oqibatlarini kamaytirish va kiberjinoyatlarni tergov qilishda xalqaro hamkorlikni kuchaytirish uchun huquqiy mexanizmlar yaratishga qaratilgan.

O‘zbekistonning kelgusida Budapesht Konvensiyasiga qo‘shilishi kiberjinoyatchilikka qarshi kurashishda yangi imkoniyatlar eshigini ochadi. Konvensiyaga a’zo bo‘lish orqali O‘zbekiston xalqaro darajada kiberxavfsizlikni ta’minlash va kiberjinoyatchilikka qarshi kurashishda ilg‘or tajriba almashish imkoniyatiga ega bo‘ladi. Shuningdek, xalqaro hamkorlik orqali kiberjinoyatlar oqibatlarini kamaytirish va kiberxavfsizlikni ta’minlashda samarali yondashuvlarni joriy qilishi mumkin.

Xulosa va takliflar

Mazkur tezisda kiberjinoyatchilikning huquqiy, texnologik va tashkiliy jihatlari tahlil qilindi. O‘zbekiston Respublikasining tegishli qonun hamda xalqaro tajribalar asosida, mamlakatda kiberjinoyatchilikka qarshi kurash choralarining kuchaytirilishi dolzarb ekanligi qayd etildi. Zamonaviy texnologiyalar, xususan sun’iy intellekt va mashinaviy o‘rganish texnologiyalari, kiberjinoyatlarni aniqlash va oldini olishda samarali vosita bo‘lib xizmat qilishi va xalqaro hamkorlik va xalqaro konvensiyalarga qo‘shilishning ahamiyati ta’kidlandi.

Takliflar

Mutaxassislar tayyorlashni kuchaytirish: Kiberxavfsizlik bo‘yicha yuqori malakali kadrlar tayyorlash uchun maxsus o‘quv dasturlari va texnologik markazlarni tashkil etish lozim.

Sun’iy intellekt texnologiyalarini joriy etish: Kiberjinoyatchilikka qarshi kurashda sun’iy intellektdan keng foydalanish, bu boradagi ilg‘or tajribalarni milliy kiberxavfsizlik tizimiga tatbiq etish.

Xalqaro hamkorlikni kuchaytirish: O‘zbekistonning Budapesht Konvensiyasiga qo‘shilishi orqali xalqaro hamkorlikni mustahkamlash va kiberjinoyatlarning oldini olishda global resurslardan foydalanish imkoniyatlarini kengaytirish.

KIBERJINOYATCHILIK, KIBERETIKA VA ULARDAN HIMOYALANISH

Raximov Sherbek Kamolovich

Malaka oshirish instituti Kasbiy tayyorgarlik fakulteti Maxsus fanlar sikli o‘qituvchisi

Yangi texnologiyalar, elektron xizmatlar bizning kundalik hayotimizning ajralmas qismiga aylandi. Jamiyat kundan-kun axborot-kommunikasiya texnologiyalariga tobora ko‘proq qaram bo‘lib borayotganligini hisobga olib, ushbu texnologiyalarni himoya qilish va ulardan foydalanish milliy manfaatlar uchun hal qiluvchi ahamiyatga ega va juda muhim mavzuga aylanmoqda.

Axborot-kommunikasiya texnologiyalar qanchalik rivojlangan sari kiberjinoyatchilik va uning turlari ham ko‘payib bormoqda.

Kiberjinoyatchilik bu – kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat turi bo‘lib, uning eng keng tarqalgan turlari - kompyuter qaroqchiligi, onlayn firibgarlik, kompyuter tizimlariga hujum qilish, shaxsiy ma’lumotlarni o‘g‘irlash va noqonuniy yoki taqiqlangan ma’lumotlarni tarqatish.

Kiberjinoyatni amalga oshirganda quyidagilar asosiy maqsad sifatida qaraladi:

- pul, qimmatli qog‘ozlar, kredit, moddiy boyliklar, tovarlar, xizmatlar, imtiyozlar, ko‘chmas mulk, yoqilg‘i xom ashyosi, energiya manbalari va strategik xom ashyolarni noqonuniy olish;
- soliq va turli yig‘imlarni to‘lashdan bosh tortish;
- jinoiy daromadlarni legallashtirish;
- qalbaki hujjatlar, shtamplar, muhrlar, blankalar, shaxsiy yutuqlar uchun kassa chiptalarini qalbakilashtirish yoki tayyorlash;
- shaxsiy yoki siyosiy maqsadlarda maxfiy ma’lumotlarni olish;
- ma’muriyat yoki ishdagi hamkasblardan shaxsiy dushmanlik munosabatlari uchun qasos olish;
- shaxsiy yoki siyosiy maqsadlar uchun mamlakat pul tizimini buzish;
- mamlakatdagi vaziyatni, hududiy ma’muriy tuzulishni beqarorlashtirish yoki siyosiy maqsadlar uchun tartibga solish;

- talonchilik, raqibni yo‘q qilish yoki siyosiy maqsadlar uchun muassasa, korxona yoki tizim ishining tartibini buzish;

- boshqa turdagi jinoyatlarni yashirish uchun;

- tadqiqot masalalarida;

- shaxsiy intelektual qobiliyat yoki ustunlikni namoyish qilish uchun.

Kiberjinoyatlar hajmini keskin oshishiga quyidagilar motiv bo‘lib xizmat qilmoqda:

- moliyaviy qiyinchilikdan chiqish;

- jinoyatchidan bo‘lgan qarzdorlikni kechikmasdan jamiyatdan olish;

- kompaniyadan va ish beruvchidan o‘ch olish;

- o‘zini tengsizligini ko‘rsatish uchun.

Kiberjinoyatlarning yana bir turi inson va fuqorolarning huquqlari va erkinliklariga qarshi jinoyatlar - “kompyuter qaroqchiligi”dir. Ushbu jinoyatlar dasturiy ta’minotni noqonuniy nusxalash, ishlatish va tarqatishda namoyon bo‘ladi. Bu dasturiy ta’minot va ma’lumotlar bazasini yaratish bilan bog‘liq huquqiy munosabatlarga (mualliflik huquqi) jiddiy zarar yetkazadi. Bundan tashqari, dasturiy ta’minot kompaniyalariga katta moliyaviy yo‘qotishlarni olib keladi.

Kiberetika – kompyuterlar bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi, umuman insonlarga va jamiyatga qanday ta’sir ko‘rsatishini o‘rganadi.

Kiberetika masalalariga quyidagi misollarni keltirish mumkin:

- Internetda boshqa odamlar to‘g‘risidagi shaxsiy ma’lumotlarni (masalan, onlayn holatlar yoki GPS orqali joriy joylashuvni) uzatish joizmi?

- foydalanuvchilarni soxta ma’lumotlardan himoya qilish kerakmi?

- raqamli ma’lumotlarga kim egalik qiladi (musiqa, filmlar, kitoblar, vebsahifalar va boshqalar) va ularga nisbatan foydalanuvchilar qanday huquqlarga ega;

- onlayn qimor va pornografiya tarmoqda qanday darajada bo‘lishi kerak?

- Internetdan foydalanish har bir kishi uchun mumkin bo‘lishi kerakmi?

Mutaxassislar kompyuterdan foydalanishda quyidagi qoidalarga amal qilish kerakligini ta’kidlaydi:

- shaxsiy kompyuteringizdan boshqalarning zarariga foydalanmang;

- boshqa foydalanuvchilarning kompyuter ishlariga xalaqit bermang;

- boshqa odamlarning kompyuter fayllariga qaramang;

- o‘g‘irlik uchun kompyuterdan foydalanmang;

- yomonlik uchun kompyuterdan foydalanmang;

- o‘z pulingizga sotib olmagan dasturdan foydalanmang va nusxa ko‘chirmang;

- birovni kompyuterini ruxsatsiz foydalanmang;

- birovlarni intellektual mehnati samarasiga zarar yetkazmang;

- siz yaratgan dasturni ijtimoiy oqibati haqida o‘ylang;

- o‘z kompyuteringizdan boshqalarga nisbatan ongli va hurmat bilan foydalaning.

Ijtimoiy (sosial) injineriya - turli psixologik usullar va firibgarlik amaliyotining to‘plami bo‘lib, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olish hisoblanadi. Maxfiy ma’lumotlar - foydalanuvchi ismi, parollari, shaxsiy ma’lumotlari, ayblov dalillari, bank karta raqamlari va moliyaviy yoki obro‘sini yo‘qotadigan har qanday ma’lumot.

Uyali telefondan foydalanuvchilarni pul o‘g‘irlashga qaratilgan firibgarlikning turli usullari mavjud. Bunga qo‘ng‘iroqlar yoki lotereyalardagi yutuqlar, SMS-xabarlar, xatolar orqali pulni qaytarish to‘g‘risida so‘rovlar yoki jabrlanuvchining yaqin qarindoshlari muammoga duch kelganligi hamda ma’lum miqdordagi pulni zudlik bilan o‘tkazish kerakligi haqidagi xabarlarni keltirish mumkin. Mazkur hollarda quyidagi xavfsizlik choralarini amalga oshirish talab etiladi:

- telefon qiluvchining shaxsini aniqlash;
- raqamni aniqlash xizmatidan foydalanish;
- SMS – xabardagi noma’lum havolalarga e’tibor bermaslik.

Kundan-kunga takomillashib ketayotgan kiberjinoyatchilikka qarshi kiberxavfsizlikni ta’minlashda quyidagi asosiy talablarni bajarish orqali ulardan himoyalanish, ya’ni kiberxavfsizlikni ta’minlashimiz mumkin:

- xodimlarga axborot xavfsizligi asoslarini o‘rgatish;
- foydalanayotgan dasturiy mahsulotlarning zaifliklarini doimiy sinovdan o‘tkazish;
- ishonchli antivirus dasturidan foydalanish;
- lisenziyalangan rasmiy dasturlardan foydalanish;
- axborot tizimlarini himoyalashda ko‘p faktorli autentifikasiyadan foydalanish;
- parollardan foydalanishda kuchli parolni saqlash siyosatiga rioya qilish;
- muntazam ravishda kompyuter qattiq disklaridagi ma’lumotlarni shifrlash.

Hozirgi kunda axborot xavfsizligi masalasi butun jahon bo‘yicha eng muhim muammodir.

Xulosa qilib shuni ta’kidlash mumkinki, kompyuter xavfsizligi o‘z qo‘limizda! Kiber o‘g‘rilardan himoyalanish uchun esa quyidagi bir necha qoidalarga amal qilish zarur:

- **birinchidan,** kompyuterda lisenziyali antivirus hamda ushbu antivirusning omborini tez-tez yangilab turish;
- **ikkinchidan,** agar server kompyuter bo‘lsa, antivirus bilan bir qatorda, har xil juda ishonchli va kuchli brandmauerlar o‘rnatib qo‘yish;
- **uchinchidan,** maxfiy so‘zlar (parol va kod)larni faqat soz yoki harf emas, balki katta harflar hamda bir necha simvollardan tashkil qilish;
- **to‘rtinchidan,** oddiy hisoblangan axborot xavfsizligiga zarar keltiruvchi narsalarni hisobga olgan holda hech qachon yuzaki ishlamaslik;
- **beshinchidan,** biror-bir yangi tizim yaratilganda, albatta, professional kompyuter mutaxassisiga tekshirtirish;
- **oltinchidan,** internetda chop etilayotgan har kungi yangi buzish va tizim zaifliklarini o‘rganish usullarini qayta ko‘rib, shu xatoliklar bizda ham bo‘lmasligini ta’milash;
- **yettinchidan,** kalit so‘zlarni kiritayotganda, begona inson ko‘rmaslik holatini tashkillashtirish.

ADABIYOTLAR RO‘YXATI:

1. O‘zbekiston Respublikasining “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonuni. 2002-yil 12-dekabr.

2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni. 2022-yil 15-aprel.
3. G‘aniev S.K, G‘aniev A.A, Xudoyqulov Z.T. Kiberxavfsizlik asoslari. –T. 2020-yil.
4. Iminov A.A. /2023/Kiberjinoyatchilikka qarshi kiberxavfsizlik. Maqola. IIV sayti. 2023-yil 28-aprel.

AXBOROT XAVFSIZLIGI HAMDA KIBERXAVFSIZLIKNI TA’MINLASH MASALALARI

Subanov Olimjon Suyarkul o‘g‘li

O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish Instituti Yuridik fanlar kafedrasi katta o‘qituvchisi

Annotatsiya: Mazkur maqolada axborot xavfsizligi hamda kiberxavfsizlikni ta’minlash masalalari yoritilgan.

Kalit so‘zlar: Axborot-siyosiy xavfsizlik, davlatning xavfsizligi, shaxsiy ma’lumotlarni himoya qilish, axborot manipulyatsiyasi va soxta ma’lumotlar, texnik himoya vositalari va bilimlar.

Bugungi kunda axborot xavfsizligi, axborot-siyosiy xavfsizlik jamiyat va xalqaro siyosiy maydondagi, shu bilan birga, insoniyat hayotidagi barqarorlikni saqlashning eng asosiy faktori tarzida bo‘y ko‘rsatmoqda. Shuningdek, dunyo siyosiy sahnasidagi tez-tez ko‘zga tashlanayotgan turli informatsion xurujlar global muammoga aylanib ulgurdi. Bu esa axborot xavfsizligi masalasi va u bilan bog‘liq muammolar hamda jarayonlarni ilmiy va amaliy tadqiq etishni taqozo etmoqda.

Yangi O‘zbekiston Respublikasi Konstitutsiyaning 33-moddasida “Har kim istalgan axborotni izlash, olish va tarqatish huquqiga ega. Davlat Internet jahon axborot tarmog‘idan foydalanishni ta’minlash uchun shart-sharoitlar yaratadi. Axborotni izlash, olish va tarqatishga bo‘lgan huquqni cheklashga faqat qonunga muvofiq hamda faqat konstitutsiyaviy tuzumni, aholining sog‘lig‘ini, ijtimoiy axloqni, boshqa shaxslarning huquq va erkinliklarini himoya qilish, jamoat xavfsizligini hamda jamoat tartibini ta’minlash, shuningdek davlat sirlari yoki qonun bilan qo‘riqlanadigan boshqa sir oshkor etilishining oldini olish maqsadida zarur bo‘lgan doirada yo‘l qo‘yiladi” deb ko‘rsatib o‘tilgan [1].

Axborot-siyosiy xavfsizlik deganda fuqarolar, davlat va jamiyatning muhim hayotiy manfaatlarini siyosiy sohada ichki va tashqi axborot tahdidlaridan himoya qilish bilan bog‘liq kompleks muammolar tushuniladi. Uni yanada yaqqolroq ifodalaydigan bo‘lsak, ular quyidagilardir: birinchidan, fuqarolar, jamiyat va davlatning manfaatlarini umum qabul qilingan xavfsizliklarini ta’minlashga qaratiladi; ikkinchidan, axbortlarning tezlik bilan rivojlanib borishi siyosiy sohada tashqi va ichki tahdidlarga qarshi axborotlardan foydalanish imkoniyatlarini izlash va topish majburiyatini yuklaydi.

Axborot xavfsizligi hozirgi zamonda har bir fuqaro, korxona va davlat uchun eng muhim va dolzarb masalalardan biri hisoblanadi. Kundalik hayotimizda internet va axborot texnologiyalari ta’siri ortib borar ekan, axborot xavfsizligi masalasi ham hayotiy ahamiyat kasb etmoqda. Biz nima uchun axborot xavfsizligiga katta e’tibor qaratishimiz kerakligini tushunish uchun quyidagi nuqtalarga diqqat qaratish lozim.

“Shaxsga doir ma’lumotlar to‘g‘risida”gi 2019-yil 2-iyul kunidagi O‘zbekiston Respublikasining O‘RQ-547-sonli qonunining 4-moddasida **Shaxsga doir ma’lumotlarga** quyidagicha ta’rif berilgan.

Shaxsga doir ma’lumotlar — muayyan jismoniy shaxsga taalluqli bo‘lgan yoki uni identifikatsiya qilish imkonini beradigan, elektron tarzda, qog‘ozda va (yoki) boshqa moddiy jismda qayd etilgan axborot [2].

Shaxsiy ma’lumotlarni himoya qilish. Bugungi kunda onlayn xizmatlardan foydalanish jarayonida biz shaxsiy ma’lumotlarimizni turli veb-saytlarga, mobil ilovalarga yoki internet-do‘konlariga kiritamiz. Agar bu ma’lumotlar yovuz niyatli shaxslarning qo‘liga tushsa, ular shaxsiy ma’lumotlarimizni o‘g‘irlashlari, bank hisoblarimizni buzib kirishlari yoki boshqa og‘ir jinoyatlarni sodir etishlari mumkin.

Birgina misol, 2017-yildagi Equifax ma’lumotlarining buzilishi natijasida 147 million fuqaroning shaxsiy ma’lumotlari o‘g‘irlangan [3]. Bu voqea ko‘plab odamlarning bank hisoblariga zarar yetkazgan va shaxsiy ma’lumotlarini himoyalash bo‘yicha yangi tartiblarni kiritishga sabab bo‘lgan.

Korxonalar uchun iqtisodiy xavf. Korxonalar uchun axborot xavfsizligi — bu nafaqat ularning ma’lumotlarini himoya qilish, balki ularning iqtisodiy barqarorligini ta’minlash masalasidir. Axborot texnologiyalari orqali amalga oshiriladigan operatsiyalar har qanday korxona uchun muhim ahamiyatga ega. Agar korxonaning ichki ma’lumotlari yomon niyatli shaxslar tomonidan o‘g‘irlansa yoki buzib kirilsa, bu nafaqat moliyaviy yo‘qotishlarga olib kelishi, balki korxonaning obro‘siga ham jiddiy zarar yetkazishi mumkin. Masalan, Yahoo kompaniyasining 2013 va 2014-yillardagi kiber hujumlar natijasida 3 milliarddan ortiq foydalanuvchining ma’lumotlari oshkor bo‘lgan [4].

Davlatning xavfsizligi. Axborot xavfsizligi davlatlar uchun ham strategik ahamiyatga ega. Davlat tuzilmalari va aholining muhim ma’lumotlari himoya qilinmasa, har xil yovuz niyatli guruhlar ulardan foydalanib, davlat tuzilmasiga zarba berishlari mumkin. Bu nafaqat milliy xavfsizlik masalasi, balki butun mamlakat barqarorligi uchun ham katta tahdiddir.

Axborot manipulyatsiyasi va soxta ma’lumotlar. Axborot xavfsizligi nafaqat ma’lumotlarni himoya qilish, balki soxta ma’lumotlarni tarqatishdan himoyalanishni ham o‘z ichiga oladi. Bugungi kunda internet va ijtimoiy tarmoqlar orqali yolg‘on axborot tarqatish juda omaalashgan. Bunday harakatni sodir etuvchi shaxslar, odatda, ommaviy axborot vositalari va ijtimoiy tarmoqlardan foydalanib, jamiyatni manipulyatsiya qilishga urinmoqdalar. Yana bir misol, bugungi kunda dunyo bo‘ylab tarqalgan har xil reklamalar. Masalan, “siz bir million pul mukofotiga ega bo‘ldingiz” degan xabarlarga ishonib, hisob raqamlaridagi pullarni yechib olish kabi holatlar qurboni bo‘lishmoqda.

Texnik himoya vositalari va bilimlar. Axborot xavfsizligi faqatgina texnik choralar bilan cheklanmaydi. Har bir inson ham axborot xavfsizligi haqida ma’lum bir

bilimlarga ega bo‘lishi kerak. Kompyuterlar va mobil qurilmalarda kuchli parollardan foydalanish, shubhali elektron pochta xabarlarini ochmaslik, ma’lumotlarni rezerv ko‘chirish kabi oddiy, ammo muhim choralar orqali shaxsiy ma’lumotlarimizni himoya qilish mumkin.

Bugungi kunda kiberxavfsizlik sohasi tez rivojlanib bormoqda, va har bir insonga axborot xavfsizligi bo‘yicha bilimlarini oshirish muhim. Masalan, xalqaro tashkilotlar va universitetlar tomonidan bepul kiberxavfsizlik kurslari tashkil etilmoqda, va bu bilimlar har bir inson uchun axborot xavfsizligini ta’minlashda muhim ahamiyatga ega.

Axborot xavfsizligi bugungi kunda har bir inson, korxona va davlat uchun hayotiy ahamiyatga ega. Shaxsiy ma’lumotlarni himoya qilish, iqtisodiy xavflarni bartaraf etish, davlat xavfsizligini ta’minlash va soxta ma’lumotlardan himoyalanish uchun axborot xavfsizligi bo‘yicha zarur choralarni ko‘rishimiz kerak. Axborot xavfsizligi sohasidagi bilimlarimiz va texnik himoya vositalaridan foydalanishimiz orqali ma’lumotlarni xavfsiz qila olamiz. Axborot xavfsizligi faqatgina texnik masala emas, balki jamiyatimizning barqarorligi va taraqqiyoti uchun muhim omildir. Bugungi kunda yurtimizda axborot xavfsizligi hamda kiberxavfsizlikni ta’minlash masalalariga alohida e’tibor qaratilmoqda. Jumladan, axborot xavfsizligi sohasida ishlab chiqilayotgan va takomillashtirilayotgan qonunlar va qonunosti hujjatlari bunga yaqqol misol bo‘la oladi.

Axborot-kommunikatsiya texnologiyalarini rivojlantirish hamda ushbu jarayonda shaxs, jamiyat va davlatning axborot xavfsizligi hamda kiberxavfsizlikni ta’minlash masalalari mamlakatning ustuvor strategik va umummilliy vazifasi hisoblanib, davlat va jamiyat tomonidan o‘zaro mushtarak, birgalikda sa’y-harakatlarni amalga oshirilishini talab etadi. Vazirlik va idoralar, korxona va tashkilotlar, biznes tuzilmalarining axborot xavfsizligi hamda kiberxavfsizlikni ta’minlash, mamlakatimizning milliy manfaatlariga xizmat qilish demakdir. Bu, ayniqsa, milliy xavfsizlikka tahdidlar axborot makoni va muhiti orqali amalga oshirilayotgan bir pallada yanada yaqqol namoyon bo‘ladi.

Kiberxavfsizlik sohasi davlat tomonidan tartibga solingan bo‘lib, “Kiberxavfsizlik to‘g‘risida”gi 2022-yil 15-aprel kunidagi O‘zbekiston Respublikasining O‘RQ-764-sonli qonunining 10-moddasida O‘zbekiston Respublikasida kiberxavfsizlik sohasidagi yagona davlat siyosatini O‘zbekiston Respublikasi Prezidenti belgilaydi deb ko‘rsatilgan [5].

O‘zbekiston Respublikasi Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organidir. O‘zbekiston Respublikasi Davlat xavfsizlik xizmatiga kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlarni va davlat dasturlarini ishlab chiqishi, kiberxavfsizlik to‘g‘risidagi qonunchilik hujjatlarining ijro etilishi ustidan nazoratni amalga oshirishi, kiberxavfsizlik hodisalari yuzasidan tezkor-qidiruv tadbirlarini, tergovga qadar tekshiruvlarni va tergov harakatlarini amalga oshirish, kiberxavfsizlik hodisalarining oldini olish, ularni aniqlash va bartaraf etish hamda ularga nisbatan tegishli chora-tadbirlarni, shu jumladan ularning oqibatlarini tugatish bo‘yicha tashkiliy-texnik chora-tadbirlarni ko‘rishi, favqulodda vaziyatlarda axborot tizimlari va resurslarini kiberhimoya qilish hamda kiberxavfsizlik sohasidagi boshqa masalalar bo‘yicha chora-tadbirlarni o‘z ichiga olgan rejalarni ishlab chiqishi, kiberxavfsizlikni ta’minlashga doir ishlarni, shuningdek muhim axborot infratuzilmasi

obektlarida kiberhujumlarning oldini olishga, ularni aniqlashga va ularning oqibatlarini tugatishga doir ishlarni tashkil etishi, muhim axborot infratuzilmasi obektlarining kiberxavfsizligini ta’minlashga doir talablarni belgilashi kabi bir qancha yangi vazifalar yuklatildi.

Kiberxafvsizlikni ta’minlash maqsadida kiberxafvsizlik subektlarining o‘z kiberxavfsizligini ta’minlash maqsadida vakolatli davlat organidan kibertahdidlar, dasturiy ta’minotdagi, uskunalar va texnologiyalardagi zaifliklar to‘g‘risidagi ma’lumotlarni olishi, kiberhujumlardan himoya qilish vositalari va usullari, shuningdek ularni aniqlash hamda bartaraf etish usullari to‘g‘risida vakolatli davlat organidan ma’lumotlar va maslahatlar olishi o‘z kiberxavfsizligini ta’minlash bo‘yicha chora-tadbirlarni ishlab chiqish va amalga oshirishi kabi huquqlari belgilandi. Shunday ekan, bu sohadagi bilimlarimiz va tajribamizga alohida e’tibor qaratishimiz zarur.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasi Konstitutsiyasi. T. 2023 https://lex.uz/docs/6445145
2. “Shaxsga doir ma’lumotlar to‘g‘risida”gi 2019-yil 2-iyul kunidagi O‘zbekiston Respublikasining O‘RQ-547-sonli qonuni. https://lex.uz/docs/4396419
3. Kreditnoe bюro Equifax vыplatit $700 mln iz-za krupneyshey utechki dannыx. https://www.interfax.ru/business/669989
4. “V Yahoo zaяvili, chto xakerskaя ataka 2013 goda zatronula 3 mlrd akkauntov” https://tass.ru/ekonomika/4614220
5. “Kiberxavfsizlik to‘g‘risida”gi 2022-yil 15-aprel kunidagi O‘zbekiston Respublikasining O‘RQ-764-sonli qonuni. https://lex.uz/uz/docs/-5960604

KIBERJINOYATCHILIKKA QARSHI KURASHISHNING ZAMONAVIY USULLARI

Ochilov Navro‘zbek O‘roqboy o‘g‘li

Jizzax viloyati Baxmal tumani IIB Jamoat xavfsizligi xizmati, huquqbuzarliklar profilaktikasi bo‘linmasi profilaktika inspektori

Annotatsiya. Maqola kiberjinoyatchilikka qarshi kurashishning zamonaviy usullarini tahlil qilishga bag‘ishlangan. Unda kiberjinoyatchilikning asosiy shakllari, axborot xavfsizligiga bo‘lgan tahdidlar va sun’iy intellekt, blockchain texnologiyasi kabi ilg‘or texnologiyalarning qo‘llanilishi ko‘rib chiqiladi. Shuningdek, maqolada huquqiy yondashuvlar va xalqaro hamkorlikning ahamiyati tahlil qilinib, amaliy tavsiyalar berilgan.

Kalit so’zlar: Kiberjinoyatchilik, axborot xavfsizligi, sun’iy intellekt, blockchain texnologiyasi, kiberxavfsizlik.

Аннотация. Статья посвящена анализу современных методов борьбы с киберпреступностью. Рассматриваются основные виды киберпреступлений, угрозы информационной безопасности, а также использование передовых технологий, таких как искусственный интеллект и технология блокчейн. В статье

также анализируется значение правовых подходов и международного сотрудничества, предлагаются практические рекомендации.

Ключевые слова: Киберпреступность, информационная безопасность, искусственный интеллект, технология блокчейн, кибербезопасность.

Abstract.The article is dedicated to analyzing modern methods of combating cybercrime. It examines the main types of cybercrime, threats to information security, and the application of advanced technologies such as artificial intelligence and blockchain technology. The article also highlights the importance of legal approaches and international cooperation, providing practical recommendations.

Key words: Cybercrime, information security, artificial intelligence, blockchain technology, cybersecurity.

Kirish. So‘nggi o‘n yilliklarda axborot-kommunikatsiya texnologiyalarining tezkor rivojlanishi inson hayotining barcha sohalariga ijobiy ta’sir ko‘rsatgan bo‘lsa-da, bu bilan birga yangi turdagi xavflar va jinoyatlar paydo bo‘lishiga sabab bo‘ldi. Ayniqsa, kiberjinoyatchilik dunyo hamjamiyatini tashvishga solayotgan dolzarb muammolardan biri sifatida ko‘zga tashlanmoqda. Bugungi kunda raqamli iqtisodiyot, davlat boshqaruvi, ta’lim va sog‘liqni saqlash kabi ko‘plab sohalarda foydalanilayotgan axborot tizimlarining zaifliklari yirik moliyaviy zararlar, ma’lumotlar maxfiyligini buzish va davlatlararo xavfsizlik muammolarini keltirib chiqarmoqda. [1,5]

Kiberjinoyatchilik faqat texnik muammo emas, balki u ijtimoiy, iqtisodiy va huquqiy oqibatlarga olib keladigan ko‘p qirrali hodisa hisoblanadi. Masalan, xalqaro tadqiqotlar ko‘rsatmoqda: har yili kiberhujumlar tufayli jahon iqtisodiyoti trillionlab dollar miqdorida zarar ko‘radi. Shu bilan birga, turli davlatlarning strategik axborotlari o‘g‘irlanishi yoki soxtalashtirilishi global xavfsizlik tizimiga tahdid solmoqda.

O‘zbekiston ham bu muammolardan chetda qolmaydi. So‘nggi yillarda mamlakatda elektron hukumat, raqamli xizmatlar va elektron tijorat rivojlanishi bilan birga kiberjinoyatlar soni ortib bormoqda. Shu sababli, kiberjinoyatchilikka qarshi kurashish O‘zbekistonning ijtimoiy va iqtisodiy barqarorligini ta’minlashda muhim ahamiyat kasb etadi. Mazkur maqola kiberjinoyatchilikning o‘ziga xos xususiyatlari va unga qarshi kurashishning zamonaviy usullari, jumladan, sun’iy intellekt, blockchain texnologiyasi va boshqa ilg‘or yondashuvlarning samaradorligini tahlil qilishga bag‘ishlangan. Shu bilan birga, ushbu muammoni hal etish bo‘yicha huquqiy va texnik asoslarning takomillashtirilishi uchun amaliy tavsiyalar ham ishlab chiqiladi. [2,8]

Mavzuga oid adabiyotlarning tahlili

Kiberjinoyatchilikka qarshi kurashish bo‘yicha xalqaro tajribalarni o‘rganish, bu borada qo‘llanilayotgan yondashuvlar va texnologiyalarni tahlil qilish tadqiqotning muhim bosqichidir. Jahon miqyosida kiberjinoyatchilikni tadqiq qilishda bir qator muhim ilmiy ishlanmalar va hisobotlar mavjud. Xususan:

1. **Xalqaro kiberxavfsizlik indekslari va hisoboti**. Xalqaro telekommunikatsiya ittifoqi (ITU) tomonidan har yili e’lon qilinadigan "Global Cybersecurity Index" (GCI) hisoboti turli davlatlarning kiberxavfsizlik sohasidagi holati va imkoniyatlarini

baholaydi. Ushbu indeks davlatlararo hamkorlik, siyosiy strategiyalar va texnologik innovatsiyalar bo‘yicha ma’lumot beradi.

2. **Kiberjinoyatchilikning huquqiy asoslari**. Budapesht konvensiyasi (2001) kiberjinoyatlarga qarshi kurashda xalqaro hamkorlikni mustahkamlashga yo‘naltirilgan ilk huquqiy hujjat bo‘lib, unda kiberjinoyat turlari, ularni tergov qilish va xalqaro hamkorlik mexanizmlari aniq belgilangan. O‘zbekiston ham mazkur konvensiyaning qoidalarini milliy qonunchilikka tatbiq qilish masalasini ko‘rib chiqmoqda.

3. **Sun’iy intellekt va kiberxavfsizlikka oid ilmiy maqolalar**. Zamonaviy tadqiqotlarda sun’iy intellekt texnologiyalarining kiberjinoyatlarni aniqlash va oldini olishdagi roli keng o‘rganilgan. Masalan, mashinaviy o‘qitish algoritmlari kiberhujumlarni real vaqt rejimida aniqlash imkonini beradi.

4. **Blockchain texnologiyasi**. Kiberjinoyatlarga qarshi kurashda blockchain texnologiyasidan foydalanish istiqbollari ham dolzarb mavzulardan biridir. Ushbu texnologiya, xususan, ma’lumotlar yaxlitligini ta’minlash, soxtalashtirishni oldini olish va tranzaktsiyalarning shaffofligini oshirishda samarali hisoblanadi.

Yuqoridagi manbalar tahlili shuni ko‘rsatadiki, kiberjinoyatchilikning oldini olish faqat texnik choralar bilan cheklanib qolmay, huquqiy, siyosiy va iqtisodiy yondashuvlarni ham o‘z ichiga olishi lozim. Aynan kompleks yondashuvlar kiberxavfsizlikni ta’minlashda yuqori samaradorlikka erishishni ta’minlaydi. [4,5]

Tadqiqot metodologiyasi

Ushbu maqolada kiberjinoyatchilikka qarshi kurashish bo‘yicha zamonaviy usullarni o‘rganishda quyidagi metodlardan foydalaniladi:

1. **Tahliliy yondashuv**. Kiberjinoyatlar bilan bog‘liq statistik ma’lumotlar va xalqaro hisobotlar o‘rganiladi. Ushbu ma’lumotlardan kiberjinoyatlarning asosiy shakllarini aniqlashda foydalaniladi.

2. **Taqqoslama usul**. Dunyoning rivojlangan mamlakatlari, xususan, AQSh, Yevropa Ittifoqi davlatlari va Osiyo mamlakatlarining tajribalari milliy yondashuvlar bilan solishtiriladi.

3. **Ekspertiza**. Kiberxavfsizlik sohasi mutaxassislari, IT-ekspertlar va huquqshunoslar bilan intervyu o‘tkazilib, amaliy takliflar ishlab chiqiladi.

4. **Amaliy tadqiqot**. Sun’iy intellekt, blockchain va boshqa zamonaviy texnologiyalarning kiberjinoyatchilikka qarshi kurashda qo‘llanilishi real misollar asosida tahlil qilinadi.

Tahlil va natijalar

Tadqiqot davomida quyidagi asosiy jihatlar aniqlangan:

1. **Kiberjinoyatlarning asosiy turlari**. Ma’lumotlarni o‘g‘irlash (data breaches), ransomware (ma’lumotlarni shifrlash va to‘lov talab qilish), phishing (firibgarlik orqali shaxsiy ma’lumotlarni qo‘lga kiritish) kabi jinoyatlar global darajada keng tarqalgan.

2. **Texnologik yondashuvlarning samaradorligi**. Sun’iy intellekt algoritmlari real vaqt rejimida tahdidlarni aniqlash va ularni avtomatik ravishda bloklash imkonini beradi. Shuningdek, blockchain texnologiyasi tranzaktsiyalarni soxtalashtirishning oldini olishda muhim rol o‘ynaydi.

3. **Huquqiy va xalqaro hamkorlik zarurati**. Milliy qonunchilikning xalqaro standartlarga mos kelmasligi kiberjinoyatlarning oldini olishda muayyan to‘siqlarni

yuzaga keltiradi. Shu sababli, xalqaro hamkorlik va ma’lumot almashish mexanizmlarini rivojlantirish zarur.

Xulosa va takliflar

1. **Huquqiy asoslarni mustahkamlash**. O‘zbekiston qonunchiligida kiberjinoyatlarni aniqlash va jazolash bo‘yicha maxsus huquqiy normalarni ishlab chiqish zarur.

2. **Kiberxavfsizlik infratuzilmasini rivojlantirish**. Zamonaviy texnologiyalar, jumladan, sun’iy intellekt va blockchain texnologiyasidan keng foydalanish kiberjinoyatchilikka qarshi samarali kurashda muhim ahamiyatga ega.

3. **Aholining kiberxavfsizlik bo‘yicha savodxonligini oshirish**. Kiberjinoyatlarning ko‘pchiligi aholining yetarli darajada axborot xavfsizligiga e’tibor bermasligi bilan bog‘liq. Shu sababli, keng ko‘lamli ta’lim dasturlarini tashkil etish zarur.

4. **Xalqaro hamkorlikni kuchaytirish**. Budapesht konvensiyasiga qo‘shilish va boshqa xalqaro tashkilotlar bilan hamkorlikni rivojlantirish muhimdir.

Foydalanilgan adabiyotlar ro‘yxati (References)

1. Xalqaro telekommunikatsiya ittifoqi (ITU). "Global Cybersecurity Index 2023".
2. Anderson R., Moore T. "The Economics of Cybercrime". Journal of Economic Perspectives, 2019, Vol. 33(1), pp. 3–20.
3. Budapesht konvensiyasi. "Kiberjinoyatlarga qarshi kurashish bo‘yicha Konventsiya", 2001.
4. Nguyen T., Hoang D. "Artificial Intelligence in Cybersecurity: Challenges and Opportunities". IEEE Transactions on Information Forensics, 2022, Vol. 17(4), pp. 54–68.
5. Nakamoto S. "Bitcoin: A Peer-to-Peer Electronic Cash System". Available online: https://bitcoin.org/bitcoin.pdf, 2008.

КИБЕРЖИНОЯТЛАРНИ ТЕРГОВ ҚИЛИШДА ИСБОТЛАНИШИ ЛОЗИМ БЎЛГАН ҲОЛАТЛАР

Эшқулов Достон Жаҳонгир ўғли

ИИВ Малака ошириш институти Юридик фандар кафедраси ўқитувчиси

Аннотация: мақолада миллий ва халқаро тажрибани таҳлил қилиш асосида ахборот технологиялари, интернет, онлайн тўлов тизимларидан фойдаланган ҳолда содир этилган кибержиноятларни тергов қилишда исботланиши лозим бўлган ҳолатлар ва уларни тергов қилишнинг хусусиятлари ёритилган.

Калит сўзлар: кибержиноят, кибержиноятларни тергов қилиш методикаси, фишинг, интернет, ахборот- коммуникация технологиялари

Шиддат билан ривожланиб бораётган дунё глобал ахборот майдонида кибер макон билан боғлиқ янгидан-янги, турли хилдаги таҳдидлар юзага

келмоқда. Замонавий дунёда бутун инсоният учун ахборот соҳасидан келаётган хавфлар, хусусан турли кибер ҳужумлар хавфи ҳамон сақланиб қолмоқда.

Ҳар бир жиноят табиатан индивидуалдир. Аммо бу алоҳида мос келадиган элементлар учун илгари қилинган ҳар қандай нарсага хос бўлиши мумкин ёки бўлмаслиги мумкин. Шу билан бирга, ҳуқуқни қўллаш амалиётидан олинган умумий билимлар маълум бир таркибни текширишда фойдали бўлиши мумкин бўлган ҳолатлар доирасини ажратиб кўрсатишга имкон беради:

1. Жиноят-протсессуал қонунининг қоидаларига кўра, ваколатли шахс ҳар қандай содир этилган ёки тайёрланаётган жиноят тўғрисидаги хабарни қабул қилиши, текшириши ва ўз ваколати доирасида қонун ҳужжатларида белгиланган муддатда қонуний ва асосли қарор қабул қилиши шарт. Бундан ташқари, аллақачон маълум бўлган жиноий фактларни тасдиқлаш ёки рад этиш учун ҳам, янгиларини аниқлаш учун ҳам. Масалан, клубнинг ноқонуний молиявий-хўжалик фаолияти тўғрисидаги хабарни дастлабки текшириш давомида қимор ўйинларини ўтказиш учун ўйин ускуналари, шунингдек, ўйин зонаси ташқарисидаги Интернет тармоғидан ноқонуний фойдаланиш фактлари аниқланди[15].

Жиноят тўғрисидаги хабарни текшириш босқичида қуйидаги ҳолатлар аниқланиши лозим:

- жиноят содир этилганлиги (кўриб чиқилаётган ҳаракат жиноятми);

- жиноий тажовуз обекти[16] (замонавий кибержиноятни таҳлил қилиб, у фақат компютер маълумотлари тизими билан чекланмайди деган хулосага келиш мумкин);

- жиноят содир этилган жой (жиноят содир этилган жойлар бир-биридан анча узоқроқ бўлиши мумкин, шунингдек, бир нечта бўлиши мумкин), зарарли оқибатлар содир бўлган жой, жиноят содир этилган вақт;

- жиноят содир этиш усули, шу жумладан кибер технологиялар роли;

-компютер тизимининг ишлаш тартиби, компютер маълумотларига кириш шартлари, ҳимоя воситалари;

- жиноят қолдирган излар;

- зарарнинг ҳажми ва сифат таркиби;

- жабрланувчининг (жисмоний ёки юридик шахснинг) ва жиноят содир этган шахснинг шахси;

- жиноят содир этишга ёрдам берадиган сабаблар ва шартлар.

Жиноят изларини аниқлаш, тузатиш ва олиб қўйиш жиноят ишини сифатли тергов қилишнинг муҳим шартидир.

Ушбу тоифадаги ишларда етказилган зарар нафақат мулкий, жисмоний ва маънавий, балки ишбилармонлик обрўсига ҳам зарар етказиши мумкин.

---

[15] Marie-Helen Maras. Computer Forensics: Cybercriminals, Laws, and Evidence. 2nd Edition. USA. Jones & Bartlett Learning, LLC. 2015. – 564 p.

[16] Рустамбаев М. Х. Курс уголовного права Республики Узбекистан //Особенная часть. – 2018. – Т. 3. – С. 83-91.

Агар жабрланувчининг шахси, қоида тариқасида, дарҳол маълум бўлса, унда жиноят содир этган шахсни аниқлаш бироз куч талаб қилади, чунки кибержиноятлар, аксарият ҳолларда, ноаниқ тоифага киради.
Ушбу ҳолатни аниқлаш, кўпроқ даражада, профилактика мақсадига эга.

2. Муайян жиноят таркиби белгиларини кўрсатадиган маълумотларнинг етарлилиги ваколатли шахс томонидан амалдаги амалиётни ҳисобга олган ҳолда баҳоланади. Шубҳасиз, дастлабки маълумотларнинг миқдори маълум бўшлиқларга эга. Дастлабки тергов жараёнида уларни тўлдириш керак. Кўриб чиқилаётган тоифадаги ишларда дастлабки текширувлар материалларининг аксарият қисмида жиноят содир этган шахс тўғрисида маълумотлар мавжуд эмас. Кўпинча жиноятнинг барча излари қайд этилмайди ва олиб қўйилмайди.

3. Дастлабки маълумотларни таҳлил қилиш ва баҳолашдан сўнг, шуни таъкидлаш керакки, унинг ҳажми бошқа композитсиялардан унчалик фарқ қилмайди, мавжуд бўшлиқларни ҳисобга олган ҳолда, тергов мақсадларини тушуниш керак. Кибержиноятлар учун улар бошқаларга ҳам хос бўлади: жиноят фактини аниқлаш, содир бўлган ҳодисанинг расмини, механизмини тиклаш, ҳуқуқбузарларни аниқлаш ва қидириш, уларнинг айбини исботлаш, зарарни қоплаш ва бошқалар). Кейинчалик, уларга эришиш усуллари ва воситалари аниқланади. Шуни ёдда тутиш керакки, бундай жиноятларни тергов қилиш, қоида тариқасида, техник воситалар, тизимлар, дастурий таъминот ва кўплаб маълумотлар билан боғлиқ бўлиб, уларнинг ҳажми ўнлаб ёки ҳатто юзлаб террабайтларда ҳисобланиши мумкин, бунинг учун махсус технологиялар ва уларни қайта ишлаш воситалари, рақамли маълумотларни таҳлил қилишнинг маълум моделлари керак. Умуман олганда, мақсадлар жиноят тўғрисидаги дастлабки маълумотлар миқдори билан белгиланади.

4. Бундан ташқари, жиноий механизмни реконструксия қилиш учун ишлатиладиган суд-тиббиёт воситалари ва усуллари (масалан, моделлаштириш усуллари, компютер симулятсияси, ўтган йиллардаги жиноий ишлар материалларини таҳлил қилиш ва бошқалар) қўлланилади. Жиноят ишини тергов қилаётган шахс мавжуд маълумотлар асосида алоқалар, коррелятсиялар ва хулосалар кетма-кетлигини тузади, жиноят ижрочилари ва буюртмачисига олиб келадиган рақамли далилларни тўплайди, бу уларнинг айбини исботлаш ва жавобгарликка тортиш имконини беради.

5. Ушбу тоифадаги жиноятлар бўйича амалга ошириладиган тезкор-қидирув тадбирлари, тергов ва протсессуал ҳаракатлар хилма-хил бўлиб, қонун ҳужжатларида белгиланганидан ташқари ҳар қандай доирада чекланмайди. Уларни муваффақиятли амалга оширишнинг калити жиноий иш бўйича тергов олиб борувчи шахснинг ваколати, шунингдек ишнинг ўзига хос обектлари билан боғлиқ ҳолда маслаҳат ёрдамининг сифати ва ўз вақтида бажарилишида ётади. Амалиёт шуни кўрсатадики, маслаҳат ёрдамини таъминлаш терговни амалга ошираётган шахсга тегишли. Бундай мутахассис айбдорлик далилларини излаш ва профессионал талқин қилиш билан

шуғулланади. Компютер технологиялари ва ахборот соҳасидаги мутахассислардан ташқари, ушбу тоифадаги жиноий ишларни тергов қилишда соҳа мутахассислари энг кўп талаб қилинади:

- молиячилар, кредит ва аудит;
- иқтисодий хавфсизлик;
- банк иши;
- фуқаролик ҳуқуқи ва жараёни;
- тиббиёт ва меҳнатни муҳофаза қилиш ва бошқалар.

Биргаликда ва келишилган иш орқали бутун жиноий занжир қайта тикланади. Шундай қилиб, кибержиноятларни тергов қилиш ишининг мазмунини қисқача таҳлил қилиб, асосий босқичларни ажратиб кўрсатиш мумкин:

- дастлабки маълумотларни олиш;
- уни таҳлил қилиш, терговнинг аниқ мақсад ва вазифаларини аниқлаш;
- уларга эришиш усуллари ва воситаларини аниқлаш (иштирокчилар доирасини аниқлаш, улар билан ўзаро муносабатларни ташкил этиш, замонавий исботлаш воситаларидан фойдаланиш имкониятини таъминлаш, дастлабки текширувдаги бўшлиқларни тўлдириш, далиллар базасини тўплаш, етказилган зарарни қоплаш, жиноят содир этишга ёрдам берадиган ҳолатларни аниқлаш, уларни бартараф этиш бўйича тавсияларни ишлаб чиқиш ва амалга ошириш)[17].

Бироқ, кибержиноятларни тергов қилиш босқичларининг мазмуни бошқалардан унчалик фарқ қилмаслигига қарамай, мақсадларга эришиш усуллари ва воситалари ҳар доим ҳам янги ва юқори технологияли эмас, уларнинг тергови жиноий иш бўйича тергов олиб борадиган кўпчилик мансабдор шахслар учун жуда қийин вазифа бўлиб қолмоқда[18]. Ушбу масалалар бўйича тергов ва суд амалиётини тизимлаштирилган умумлаштиришнинг йўқлиги, терговни ташкил этиш ва ўтказиш бўйича услубий тавсияларнинг етишмаслиги ва ўз вақтида бажарилмаслиги, маълум маълумот манбалари билан ишлашнинг кам тажрибаси, шунингдек, бундай мутахассисларни тайёрлашнинг этарли эмаслиги каби омиллар билан боғлиқ бўлиши мумкин.

Фойдаланилган адабиётлар:

1. Marie-Helen Maras. Computer Forensics: Cybercriminals, Laws, and Evidence. 2nd Edition. USA. Jones & Bartlett Learning, LLC. 2015. – 564 p.
2. Рустамбаев М. Х. Курс уголовного права Республики Узбекистан //Особенная часть. – 2018. – Т. 3. – С. 83-91.
3. Sean E. Goodison, Robert C. Davis, and Brian A. Jackson. “Digital Evidence and U.S. Criminal Justice System”. The National Institute of Justice, U.S. Department of Justice. 2014. – p. 31.
4. Берова Д.М. Расследование киберпреступлений. –М. – 2018., -С.175

[17] Sean E. Goodison, Robert C. Davis, and Brian A. Jackson. “Digital Evidence and U.S. Criminal Justice System”. The National Institute of Justice, U.S. Department of Justice. 2014. – p. 31.
[18] Берова Д.М. Расследование киберпреступлений. –М. – 2018., -С.175

КИБЕРЖИНОЯТЧИЛИККА ҚАРШИ КУРАШИШ БЎЙИЧА ДОЛЗАРБ МУАММО ВА УЛАРНИНГ ЕЧИМИ

Эшқулов Достон Жаҳонгир ўғли

ИИВ Малака ошириш институти Юридик фандар кафедраси ўқитувчиси

Аннотация: мақолада кибержиноят тушунчаси ва ушбу турдаги жиноятларнинг содир этилишига имкон берган шарт-шароитлар, уларни бартараф этиш усуллари, ушбу турдаги жиноятларни олдини олиш мақсадида қандай чора тадбирлар амалга ошириш зарурлиги ёритилган.

Калит сўзлар: кибержиноят, хакерлик, фишинг, Денонсацион ҳужум, кибертерроризм, интернет, ахборот- коммуникация технологиялари

Кибержиноят тушунчаси замонавий дунёда тобора аҳамият касб этмоқда. Ҳозирги даврда интернет ва ахборот технологиялари барча соҳаларга чуқур сингиб борган бир шароитда, бу технологиялардан ноқонуний мақсадларда фойдаланиш ортиб бормоқда. Кибержиноятларнинг таҳлили, уларнинг олдини олиш ва ҳуқуқий чора-тадбирларни ишлаб чиқиш бугунги кунда жуда долзарб масала ҳисобланади.

Кибержиноятчилик ахборот технологиялари ва интернет инфратузилмаси орқали содир этиладиган жиноятлар йиғиндисини ифодалайди. Замонавий рақамли иқтисодиёт ривожланган сари, кибержиноятчилик нафақат шахсий маълумотлар, молиявий ресурслар, балки давлат ва халқаро институтлар хавфсизлигига ҳам жиддий таҳдид солмоқда. Бу каби жиноятларга қарши самарали курашиш учун халқаро ва миллий ҳуқуқий асосларни шакллантириш ва уларни доимий такомиллаштириш муҳим аҳамиятга эга.

Кибержиноят – бу ахборот технологияларидан фойдаланган ҳолда содир этилган жиноят бўлиб, у қонунлар билан ман этилган ҳаракат ёки ҳаракатсизликни ўз ичига олади. Кибержиноятлар турли кўринишларда намоён бўлиши мумкин: яъни ахборот тизимлари, шахсий ёки корпоратив маълумотларга ҳужум қилиш, фирибгарлик, инсонларнинг шахсий ҳаётига аралашиш, рақамли активларни ўғирлаш каби жиноятлар, хакерлик ҳужумлари, шахсий маълумотларни ўғирлаш, компьютер дастурларига зарар етказиш, шантаж ва бошқалар.

Замонавий ахборот жамиятида кибержиноятлар нафақат шахсларга, балки бизнес субъектлари, давлат ташкилотлари ва халқаро ҳамжамиятга катта таҳдид солмоқда. Масалан:

1. Хакерлик ҳужумлари орқали давлат ахборот тизимларига зарар етказилиши миллий хавфсизликка таҳдид солиши мумкин.
2. Банк маълумотлари ва шахсий идентификация маълумотларининг ўғирланиши кўплаб молиявий оқибатларга олиб келади.

Профессор Жон Смит таъкидлаганидек: *"Кибержиноятлар – бу янги даврнинг қотил қуроли, улар нафақат молиявий зарар етказади, балки инсонлар ва давлатлар ўртасидаги ишончни пасайтиради."*

Олимларнинг таъкидлашича, кибержиноятлар тушунчаси нафақат ахборот технологияларини ноқонуний мақсадларда қўллашни, балки ижтимоий ҳамда иқтисодий оқибатларни ўз ичига олади. Масалан, Т. Столл ўзининг асарларидан бирида қуйидагича таъкидлайди: *"Кибержиноятлар нафақат шахсий маълумотларни йўқотиш хавфини келтириб чиқаради, балки глобал иқтисодий мувозанатга ҳам таҳдид солади."*

Йилдан-йилга жиноятларнинг турлари ортиб бораётган каби кибержиноятларнинг ҳам турли кўринишлари намоён бўлмоқда. Кибержиноятларнинг энг асосий турлари сифатида қуйидагиларни кўриб чиқишимиз мумкин:

1. Хакерлик ҳужумлари (Hacking Хакерлик – бу компьютер тизимларига ноқонуний кириб боришидир ва унинг мақсади турлича бўлиб:

-Маълумотларни ўғирлаш.

-Тизимни блокировка қилиш ва гаров эвазига очиш (Ransomware).

-Маълумотларни ўзгартириш ёки йўқ қилиш.

2. Фишинг (Phishing) Фишинг – шахсий ёки молиявий маълумотларни фирибгарлик йўли билан олиш учун электрон хатлар, сайтлар ёки хабарлардан фойдаланишидир ва бунга мисол сифатида қуйидагиларни кўриш мумкин:

-Банк маълумотларини ўғирлаш.

-Шахснинг логин ва паролларини олиш.

3. Денонсацион ҳужумлар (DDoS – Distributed Denial of Service) хакерлар компьютер тармоқларига ортиқча юкламалар ташлаб, уларни ишдан чиқаради. Бу кўпинча корпорациялар ёки давлат тизимларига қарши қўлланилади.

4. Зарарли дастурлар тарқатиш (Malware) бўлиб, турли хил кўринишларда бўлади, жумладан вируслар, троянлар ва шпиён дастурлар. Уларнинг мақсади:

-Маълумотларни ўғирлаш.

-Тизимни зарарлаш.

-Фойдаланувчиларнинг фаолиятини кузатиш.

5. Кибертерроризм эса террорчилик ҳаракатлари доирасида ахборот тизимларига ҳужум қилишдир. Масалан, стратегик аҳамиятга эга давлат объектларига ҳужум қилиш орқали давлат иқтисодиётини заифлаштиришни мисол қилиб олсак бўлади.

Ҳар бир содир этилаётган ҳуқуқбузарликлар ёки жиноятларни содир этилишига қандайдир шарт-шароитлар сабаб бўлгани каби кибержиноятлар ҳам пайдо бўлиши қуйидаги бир қатор сабабларни келтириб ўтишимиз мумкин:

1. Йилдан-йилга технологиялар замонавийлашиб, мураккаблашиб бораётгани, уларни назорат қилишни қийинлаштиради ва натижада кибержиноятларнинг содир этилишига имкон яратиб беради.

2. Агар хавфсизлик яхши таъминланган бўлса ҳар қандай турдаги ва кўринишдаги ҳуқуқбузарликлар ва жиноятлар олди олиниши хеч кимга сир эмас. Баъзи бир компаниялар ва фойдаланувчилар ахборот хавфсизлигига етарлича эътибор қаратмаётганлиги ва хавфсизликнинг етарлича таъминланмаганлиги оқибатида ҳам кибержиноятлар содир этилмоқда.

3. Аксарият мамлакатларда содир этилаётган кибержиноятларга қарши ҳуқуқий меъёрларнинг етарли даражада ривожланмаганлиги, кибержиноятга қарши қонунчилик ҳали такомиллашмаганлиги ҳам айнан ўша мамлакатда кибержиноятларнинг содир этилишига шарт шароит яратиб бермоқда.

4. Ҳар бир ҳуқуқбузарлик ёки жиноятларнинг содир этилиши замирида моддий ёки номоддий манфаатлар ётади. Содир этилаётган кибержиноятларнинг асосий мақсади молиявий манфаатдорлик деб ҳисобласак муболаға бўлмайди.

Содир этилаётган кибержиноятлар жамият ва иқтисодиётга катта зарар етказиши, молиявий йўқотишлар, шахсий маълумотларнинг ошкор бўлиши, компаниялар обрўсининг тушиши ва ахборот тизимларининг ишдан чиқиши каби оқибатлар билан бирга нафақат молиявий зарар, балки ижтимоий ва психологик зарарларни ҳам қамраб олиши хеч кимга сир эмас:

- олиб борилган тадқиқотларга кўра, ҳар йили кибержиноятлар натижасида компаниялар ва шахслар миллиардлаб доллар йўқотиши Молиявий зарар ҳисобланса,

- Киберхавфсизлик муаммолари одамлар ва ташкилотлар ўртасида Ижтимоий ишончнинг пасайишига олиб келади ва психологик босим натижасида киберқурбонлар кўпинча руҳий стрессга тушади, уларда хавфсизлик ҳисси йўқолади.

Кибержиноятларнинг олдини олиш бўйича қуйидаги бир қатор чора-тадбирлар муҳим ҳисобланади:

1. **Хавфсизлик тизимларини такомиллаштириш**, яъни ахборот технологиялари тизимларига кучли ҳимоя воситаларини жорий қилиш.

2. **Ҳуқуқий меъёрларни кучайтириш**, яъни кибержиноятларга қарши халқаро даражада ҳамкорлик қилиш ва қонунларни такомиллаштириш.

3. **Аҳолини хабардор қилиш**, яъни одамларнинг ахборот хавфсизлиги бўйича билимларини ошириш.

4. **Сунъий интеллект ва аналитик воситалардан фойдаланиш**, яъни ҳужумларни олдиндан аниқлаш ва таҳлил қилиш учун замонавий технологияларни қўллаш.

5. **Халқаро ҳамкорлик**: Кибержиноятларга қарши курашда давлатлар ўртасида ҳамкорликни кучайтириш.

Доктор Элизабет Грейнинг таъкидича: *"Кибержиноятларнинг олдини олишда профилактик чоралар муҳим аҳамиятга эга. Бунинг учун ҳар бир шахс ва ташкилот хавфсизлик маданиятини шакллантириши лозим."*

Кибержиноятларни олдини олишда жамоавий ҳамкорликнинг ҳам аҳамияти шундаки кибержиноятчиликка қарши самарали кураш давлат ва хусусий секторнинг ҳамкорлиги орқали амалга оширилиши мумкин:

- Ахборот хавфсизлиги бўйича миллий марказларнинг ташкил этилиши.

- Ҳуқуқ-тартибот органлари, интернет провайдерлари ва банк секторининг ўзаро ҳамкорлиги.

- Жамоатчилик ўртасида киберхавфсизлик бўйича билимлар ва маданиятни ошириш.

Хулоса сифатида шуни таъкидлаш жоизки, кибержиноятларга қарши самарали курашиш учун ҳуқуқий асосларни такомиллаштириш, замонавий технологияларни қўллаш ва жамоатчиликни хабардор қилиш муҳим аҳамиятга эга. Бундан ташқари, давлатлар ўртасида ҳамкорликни кучайтириш орқали трансмиллий кибержиноятларнинг олдини олиш ҳам муҳимдир.

Тадқиқотчи Д.А.Брауннинг таъкидлашича *"Кибержиноятчиликка қарши кураш – бу нафақат ҳуқуқий масала, балки жамият хавфсизлигини таъминлашнинг ажралмас қисми."*

Фойдаланилган адабиётлар:

1. Каспаров М. А. (2020). *Киберхавфсизлик: назария ва амалиёт*. Москва: Юридик нашриёт.
2. Столл, К. А. (2018). *Кибержиноятчилик: муаммолар ва таҳлил усуллари*. Нью-Йорк: IT Press.
3. Жумаев Б. И. (2022). "Кибержиноятларни тергов қилиш: муаммо ва ечимлар". Онлайн манба
4. Миллер Р. Т. (2021). *Трансмиллий кибержиноятчилик: ҳуқуқий ҳимоя муаммолари*. Лондон: Cambridge Press.
5. Аҳмедов Ш. Ҳ. (2020). "Кибержиноятларга қарши кураш: Ўзбекистон тажрибаси". Ахборот хавфсизлиги журнали.

КИБЕРЖИНОЯТЧИЛИККА ҚАРШИ КУРАШИШ: МУАММОЛАР ВА ЕЧИМЛАР

Тўраев Фаррух Ҳаким ўғли

Ўзбекистон Республикаси Ички ишлар вазирлиги Малака ошириш институти жисмоний тайёргарлик цикли катта ўқитувчиси

farruxtorayev555@gmail.com

Аннотация: Мақолада кибержиноятчиликнинг моҳияти, асосий турлари ва унинг жамият ҳамда давлат учун хавфи таҳлил қилинади. Кибержиноятчиликка қарши курашишда учрайдиган ҳуқуқий, ташкилий, молиявий ва технологик муаммолар ўрганилади ҳамда уларни бартараф этиш бўйича ечимлар таклиф этилади. Хусусан, миллий қонунчиликни такомиллаштириш, халқаро ҳамкорликни кучайтириш, киберхавфсизлик соҳасидаги кадрларни тайёрлаш ва замонавий ҳимоя технологияларини жорий этиш масалаларига алоҳида эътибор қаратилади. Мақолада келтирилган ёндашувлар киберхавфсизликни таъминлаш ва кибержиноятчиликка қарши курашда самарали чора-тадбирларни амалга оширишга йўналтирилган.

Калит сўзлар: кибержиноятчилик, ахборот хавфсизлиги, киберхавф, ҳуқуқий муаммолар, ташкилий чоралар, молиявий муаммолар, технологик ечимлар, халқаро ҳамкорлик, киберхавфсизлик марказлари, сунъий интеллект.

БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ: ПРОБЛЕМЫ И РЕШЕНИЯ

Тураев Фаррух Хаким угли

Старший преподаватель цикла физической подготовки Институт повышения квалификации МВД Республики Узбекистан

farruxtorayev555@gmail.com

Аннотация: В статье анализируется сущность, основные виды киберпреступности и ее опасность для общества и государства. Изучены правовые, организационные, финансовые и технологические проблемы, возникающие при борьбе с киберпреступностью, и предложены пути их устранения. В частности, особое внимание будет уделено совершенствованию национального законодательства, укреплению международного сотрудничества, подготовке кадров в сфере кибербезопасности, внедрению современных технологий защиты. Представленные в статье подходы направлены на обеспечение кибербезопасности и реализацию эффективных мер борьбы с киберпреступностью.

Ключевые слова: киберпреступность, информационная безопасность, киберриск, правовые проблемы, организационные меры, финансовые проблемы, технологические решения, международное сотрудничество, центры кибербезопасности, искусственный интеллект.

COMBATING CYBERCRIME: PROBLEMS AND SOLUTIONS

Turaev Farrukh Hakim ugli

Senior teacher of physical training cycle

Institute for Advanced Studies of the Ministry of Internal Affairs of the Republic of Uzbekistan

farruxtorayev555@gmail.com

Abstract: The article analyses the essence, main types of cybercrime and its danger for society and the state. Legal, organisational, financial and technological problems arising in the fight against cybercrime are studied and ways to eliminate them are proposed. In particular, special attention will be paid to improving national legislation, strengthening international cooperation, training personnel in the field of cyber security, and introducing modern defence technologies. The approaches presented in the article are aimed at ensuring cybersecurity and implementing effective measures to combat cybercrime.

Keywords: cybercrime, information security, cyber risk, legal problems, organisational measures, financial problems, technological solutions, international cooperation, cybersecurity centres, artificial intelligence.

КИРИШ. Кибержиноятчилик - бу ахборот технологиялари ва интернет орқали содир этиладиган жиноятлар мажмуидир. У ахборот хавфсизлигига путур етказади, шахсий маълумотларнинг ўғирланиши, молиявий фирибгарликлар, давлат ахборот тизимларига ҳужумлар ва яна бошқа кўплаб таҳдидлар билан намоён бўлади. Ҳозирги глобаллашув ва рақамлаштириш даврида кибержиноятчилик нафақат алоҳида шахслар, балки бутун давлатлар учун катта хавф туғдирмоқда. Ушбу мақолада кибержиноятчиликнинг асосий турлари, унга қарши курашишдаги муаммолар ва ечимлар таҳлил қилинади.

Кибержиноятчилик ахборот технологияларидан фойдаланган ҳолда содир этиладиган жиноятлардир. Унинг асосий хусусияти шундаки, у жиноятни содир этишда компьютер, смартфон, сервер ёки интернет тармоғи каби воситалардан фойдаланилади. Кибержиноятларни қуйидаги турларга ажратиш мумкин:

✓ *Шахсий маълумотларнинг ўғирланиши.* Кибержиноятчилар шахсий ёки молиявий маълумотларни ўғирлаб, улардан ноқонуний фойдаланадилар. Бунга банк карталари маълумотлари, пароллар ёки шахсий идентификация маълумотлари мисол бўлади.

✓ *Киберҳужумлар.* Бу ҳужумлар давлат, хусусий сектор ёки шахсий ахборот тизимларига қаратилган бўлиб, маълумотларни бузиш, ўғирлаш ёки тизимни ишдан чиқариш мақсадида амалга оширилади. DDoS-ҳужумлари, хакерлик ва зарарли дастурлар тарқатиш бу турга киради.

✓ *Молиявий фирибгарликлар.* Онлайн тўлов тизимлари, криптовалюта савдоси ва “e-tijorat” платформалари орқали фирибгарликлар кибержиноятчиликнинг энг кенг тарқалган кўринишларидан биридир.

✓ *Рақамли шантаж.* Киберҳужумчилар маълумотларни шифрлаб (ransomware) ёки ўғирлаб, уларни қайтариш учун товон талаб қилишади.

✓ *Давлат ахборот тизимлари ва стратегик объектларга ҳужумлар.* Бу турдаги кибержиноятчилик миллий хавфсизликка таҳдид солади ва давлат органлари ҳамда стратегик объектларнинг ишлаш қобилиятига таъсир қилади.

Кибержиноятчиликка қарши курашиш кўплаб қийинчиликларни ўз ичига олади. Улар ҳуқуқий, ташкилий, молиявий ва технология билан боғлиқ муаммоларни ўз ичига олади.

Ҳуқуқий муаммолар:

Кўп давлатларда кибержиноятчиликка қарши махсус қонунлар мавжуд эмас ёки улар ҳали ривожланмаган. Кибержиноятчилик кўпинча трансмиллий бўлиб, бир давлатда содир этилиб, бошқа давлатларга зарар етказади. Бу эса ҳуқуқий ҳамкорликни қийинлаштиради. Технологиялар жуда тез ривожланади, лекин қонунларнинг янгиланиш суръати паст.

Ташкилий муаммолар:

Давлат ва хусусий сектор ўртасида хавф-хатарлар ҳақида ахборот алмашинуви етарли эмас. Шунингдек, киберхавфсизлик бўйича юқори малакали кадрлар тайёрлаш борасида жиддий муаммолар мавжуд.

Молиявий муаммолар:

Киберхавфсизликка етарли даражада маблағ ажратилмаслиги жиноятларга қарши самарали курашишга тўсқинлик қилади. Бундан ташқари кибержиноятлар

кўпинча катта молиявий зарар келтиради, лекин бундай зарарни қоплаш механизмлари ривожланмаган.

Технологик муаммолар:

Кўплаб ахборот тизимлари етарлича ҳимоя қилинмаган, шу билан бирга замонавий киберҳужумларга қарши курашиш учун кўп ташкилотларда замонавий технологиялар мавжуд эмас.

Кибержиноятчиликка қарши самарали курашиш учун қуйидаги чора-тадбирларни амалга ошириш зарур:

Ҳуқуқий чоралар:

✓ Махсус қонунларни қабул қилиш: ҳар бир давлат кибержиноятчиликка қарши қонунчилик базасини мустаҳкамлаши керак. Масалан, шахсий маълумотларни ҳимоя қилиш, киберҳужумлар учун жазо чораларини кучайтириш.

✓ Халқаро ҳамкорлик: давлатлар ўртасида ахборот алмашиш, жиноятчиларни экстрадиция қилиш ва биргаликдаги киберхавфсизлик тадбирларини ўтказиш механизмларини кучайтириш.

✓ Қонунларнинг янгиланиши: янги таҳдидларни ҳисобга олган ҳолда қонунчилик доимий равишда янгиланиши керак.

Ташкилий чоралар:

✓ Киберхавфсизлик марказларини ташкил этиш: миллий ва минтақавий даражада киберхавфсизлик марказлари яратиш орқали таҳдидларга тезкор жавоб бериш тизимини шакллантириш.

✓ Мутахассислар тайёрлаш: киберхавфсизлик соҳасида мутахассисларни тайёрлаш учун махсус ўқув дастурлари ва курсларни ташкил этиш.

Молиявий чоралар:

✓ Сармояларни ошириш: давлат ва хусусий сектор киберхавфсизлик технологияларига сармоя ажратишни кўпайтириши зарур.

✓ Сугурта тизими: кибержиноятлардан кўрилган зарарни қоплаш учун суғурта механизмларини жорий этиш.

Технологик чоралар:

✓ Замонавий ҳимояни жорий этиш: ахборот тизимлари ва тармоқларини ҳимоя қилиш учун шифрлаш, аутентификация ва бошқа замонавий технологиялардан фойдаланиш.

✓ Сунъий интеллектдан фойдаланиш: киберхавф-хатарларни аниқлаш ва уларга жавоб бериш учун сунъий интеллект ва машинали ўқитиш технологияларини жорий этиш.

ХУЛОСА. Кибержиноятчилик бугунги кунда жамият, давлат ва хусусий сектор учун энг жиддий таҳдидлардан бири ҳисобланади. Унга қарши курашиш учун ҳуқуқий, ташкилий, молиявий ва технологик ечимлар мажмуини ишлаб чиқиш зарур. Давлатлар ўртасидаги ҳамкорликни кучайтириш, киберхавфсизликни таъминлаш учун инвестицияларни кўпайтириш ва замонавий технологияларни жорий этиш орқали кибержиноятчиликка қарши самарали курашиш мумкин. Бу нафақат жиноятларни камайтиришга, балки жамиятнинг умумий хавфсизлиги ва барқарорлигини таъминлашга ёрдам беради.

АДАБИЁТЛАР

1. Шмелёв В.В. “Киберҳуқуқ: Ахборот хавфсизлигини таъминлашда ҳуқуқий ёндашувлар.” Москва, 2022.
2. Голованов С.А., ва бошқалар. “Зарарли дастурлар ва уларга қарши ҳимоя технологиялари.” Санкт-Петербург, 2021.
3. Абдураҳмонов Ш.А. “Ўзбекистонда киберхавфсизлик бўйича ҳуқуқий чора-тадбирлар.” Тошкент, 2022.
4. Ўзбекистон Республикаси Президентининг фармони. “Ахборот хавфсизлигини таъминлаш ва киберҳужумларга қарши кураш чора-тадбирлари тўғрисида.” 2022 йил.
5. Аҳмедов, Б.К. “Кибержиноятчиликнинг иқтисодий оқибатлари ва уларни бартараф этиш йўллари.” Тошкент, 2021.
6. “Telekommunikatsiya Axborot-komunikatsiya texnologiyalarida kiberxavfsizlikni ta’minlash usullari va vositalari”: xalqaro ilmiy-amaliy anjuman maqolalar to‘plami - Toshkent: O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti, 2022.

ТАЪЛИМ ТИЗИМИДА КИБЕРХАВФСИЗЛИК БЎЙИЧА КАДРЛАР ТАЙЁРЛАШ МУАММОЛАРИ

Тўраев Фаррух Ҳаким ўғли

Ўзбекистон Республикаси Ички ишлар вазирлиги Малака ошириш институти жисмоний тайёргарлик цикли катта ўқитувчиси

farruxtorayev555@gmail.com

Аннотация: Ушбу мақолада таълим тизимида киберхавфсизлик бўйича кадрлар тайёрлашнинг долзарблиги, ушбу жараёнда учрайдиган муаммолар ва уларнинг ечимлари таҳлил қилинган. Таълим дастурларининг етишмовчилиги, моддий-техник база камчиликлари, педагог кадрлар танқислиги каби масалалар атрофлича ёритилган. Шунингдек, киберхавфсизлик соҳасида юқори малакали мутахассисларни тайёрлаш учун амалга оширилиши зарур бўлган чора-тадбирлар таклиф этилган. Мақола киберхавфларга қарши курашда таълим тизимининг ўрнини мустаҳкамлашга қаратилган.

Калит сўзлар: киберхавфсизлик, кадрлар тайёрлаш, таълим тизими, педагог кадрлар, моддий-техник база, ахборот маданияти, кибержиноятчилик, замонавий технологиялар, халқаро ҳамкорлик, этика.

ПРОБЛЕМЫ ПОДГОТОВКИ КИБЕРБЕЗОПАСНОСТИ В СИСТЕМЕ ОБРАЗОВАНИЯ

Тураев Фаррух Хаким угли

Старший преподаватель цикла физической подготовки Институт повышения квалификации МВД Республики Узбекистан

farruxtorayev555@gmail.com

Аннотация: В данной статье анализируется актуальность подготовки кадров по вопросам кибербезопасности в системе образования, проблемы, возникающие в этом процессе и пути их решения. Подробно освещены такие вопросы, как отсутствие образовательных программ, отсутствие материально-технической базы, нехватка педагогических кадров. Также предложены меры, которые необходимо реализовать для подготовки высококвалифицированных специалистов в области кибербезопасности. Статья направлена на усиление роли системы образования в борьбе с киберугрозами.

Ключевые слова: кибербезопасность, подготовка кадров, система образования, педагогические кадры, материально-техническая база, информационная культура, киберпреступность, современные технологии, международное сотрудничество, этика.

CHALLENGES OF CYBERSECURITY TRAINING IN THE EDUCATION SYSTEM

Turaev Farrukh Hakim ugli

Senior teacher of physical training cycle Institute for Advanced Studies of the Ministry of Internal Affairs of the Republic of Uzbekistan

farruxtorayev555@gmail.com

Abstract: This article analyses the relevance of cyber security training in the education system, the problems arising in this process and ways to solve them. Such issues as lack of educational programmes, lack of material and technical base, shortage of teaching staff are covered in detail. Measures to be implemented to train highly qualified specialists in the field of cyber security are also proposed. The article is aimed at strengthening the role of the education system in the fight against cyber threats.

Key words: cyber security, training, education system, teaching staff, material and technical base, information culture, cybercrime, modern technologies, international cooperation, ethics.

КИРИШ. Рақамли технологияларнинг жадал ривожланиши киберхавфсизлик соҳасида юқори малака ва кўникмаларга эга кадрларга бўлган эҳтиёжни оширди. Ахборот тизимлари ва маълумотларнинг хавфсизлигини таъминлаш бугунги кунда нафақат ташкилотлар, балки давлатнинг стратегик вазифаларидан бирига айланган. Шу сабабли, таълим тизимида киберхавфсизлик бўйича кадрлар тайёрлаш масаласи кун тартибида муҳим ўрин эгаллайди. Ушбу мақолада киберхавфсизлик мутахассислари тайёрлаш жараёнидаги муаммолар ва уларнинг ечимлари муҳокама қилинади.

Киберхавфсизлик кадрлари тайёрлашнинг долзарблиги.

1. Мақсад ва аҳамият: Киберхавфлар тобора кўпайиб, замонавий иқтисодиёт ва давлат хавфсизлиги учун жиддий таҳдид солмоқда. Киберхавфларга қарши курашиш учун мутахассислар етишмовчилиги халқаро ва маҳаллий даражада сезилмоқда.

2. Таълимнинг асосий мақсадлари: Киберхавфсизлик соҳасидаги илғор технология ва воситаларни қўллай оладиган мутахассисларни тайёрлаш. Ҳар томонлама тайёрланган, амалий ва назарий билимга эга кадрларни етиштириш.

Муаммолар таҳлили.

1. Таълим дастурларининг етишмовчилиги: Киберхавфсизликка ихтисослашган махсус таълим дастурлари жуда кам. Амалиётга йўналтирилган фанларнинг камлиги мутахассисларнинг етарли даражада тайёрланмаслигига олиб келади.

2. Мутахассислар ва педагоглар танқислиги: Ахборот технологиялари соҳасида билимга эга педагоглар етишмайди. Ҳозирги ўқитувчилар киберхавфсизликнинг тезкор ўзгарувчан тенденцияларини қоплай олмайди.

3. Молиявий ва моддий база: Лабораториялар ва симуляция воситаларининг йўқлиги. Ўқув қўлланмаларнинг замонавий талабларга жавоб бермаслиги.

4. Маънавий-ахлоқий масалалар: Ёшлар орасида кибержиноятларга қизиқишнинг ошиб бориши. Ахборот хавфсизлигини таълимда ўқитишнинг этик ва ахлоқий жиҳатлари етарлича ёритилмаган.

Муаммоларнинг ечимлари.

1. Махсус таълим дастурларини яратиш: Университетларда киберхавфсизлик бўйича алоҳида факультетлар очиш. Ишлаб чиқариш ва амалиётга йўналтирилган курсларни жорий қилиш.

2. Ҳамкорлик ва тажриба алмашинуви: Халқаро даражадаги сертификат дастурлари ва тренингларни киритиш. Давлат ва хусусий сектор билан ҳамкорликда кадрларни тайёрлаш.

3. Молиявий қўллаб-қувватлаш: Таълим муассасаларини замонавий лабораториялар билан таъминлаш. Киберхавфсизлик бўйича илмий изланишларни молиялаштириш.

4. Ахборот маданияти ва этикага ўргатиш: Мактаблар ва коллежларда ахборот хавфсизлиги маданиятини шакллантириш. Ёшлар ўртасида киберхавфларнинг салбий оқибатлари ҳақида тарғибот ишларини кучайтириш.

ХУЛОСА

Киберхавфсизлик мутахассислари тайёрлаш нафақат таълим тизимидаги, балки давлат ва жамият даражасидаги стратегик вазифа ҳисобланади. Ҳуқуқий ва молиявий қўллаб-қувватлаш, педагог кадрларнинг малакасини ошириш ва янги технологияларни жорий этиш орқали бу соҳадаги муаммоларни самарали ҳал қилиш мумкин. Бу ўз навбатида мамлакатнинг рақамли хавфсизлиги ва иқтисодий барқарорлигини таъминлашга ҳисса қўшади.

ТАВСИЯЛАР

✓ Ҳар бир университетда киберхавфсизлик бўйича мутахассисликлар очиш;

✓ Дастурчилар ва киберхавфсизлик мутахассислари ўртасидаги алоқаларни кучайтириш;

✓ Киберхавфлар ҳақидаги маълумотларни аҳолига кенг ёйиш.

АДАБИЁТЛАР

1. http://psyfactor.org/lib/vershinin4.htm.
2. Абдуллаев Ш.Р. “Киберхавфсизлик асослари.” Тошкент, Ўзбекистон миллий университети нашри, 2021.
3. Каримов А.Ҳ. “Рақамли иқтисодиётда киберхавфлар: таҳдидлар ва ечимлар.” Иқтисодиёт ва инновациялар журнали, 2022.
4. Ҳасанова М.С. “Ахборот хавфсизлиги ва таълим: назарий ва амалий ёндашувлар.” Ахборот технологиялари илмий журнали, 2020.
5. Павлов Д.В. “Роль образования в борьбе с киберугрозами.” Центр инноваций и безопасности, Москва, 2020.

БУГУНГИ КУНДА КИБЕРЖИНОЯТЧИЛИКНИНГ ТАҲДИДИ ВА УНДАН ҲИМОЯЛАНИШ УСУЛЛАРИ

Бейсенов Кенжабай Сарсанбаевич

Малака ошириш институти Касбий тайёргарлик факультети Махсус фанлар цикли ўқитувчиси

Аннотация: Мазкур мақолада бугунги кунда кибер жиноятчиликнинг таҳдиди ва ундан ҳимояланиш усуллари бўйича илмий асосланган таклиф ва тавсиялар берилган.

Аннотация: В данной статье представлены научно обоснованные предложения и рекомендации об угрозе киберпреступности и способах защиты от нее на сегодняшний день.

Abstract: this article presents scientifically based proposals and recommendations on the threat of cybercrime and ways to protect against it today.

Таянч сўзлар: Киберхавфсизлик, кибержиноятчилик, киберхавфсизлик объекти, киберҳужум, кибертаҳдид, интернет.

Ключевые слова: кибербезопасность, киберпреступность, объект кибербезопасности, кибератака, кибератака в Интернете.

Base words: cybersecurity, cybercrime, cybersecurity object, cyberattack, cyberattack, internet.

Бугун технологиялар тобора ривожланиб боргани сари жиноятчилар ҳам улардан фойдаланиб, ноқонуний хатти-ҳаракатларни содир этаётир. Хусусан, одамлар карточкаларидан пулларни ўмариш сезиларли даражада ошди. Табиийки, ҳуқуқни муҳофаза қилувчи органлар томонидан бу жиноятчилар аниқланиб, тегишли жазо чоралари кўрилмоқда ва жабрланувчиларга зарар ундириб берилмоқда[19].

Бугунги кунда кибер жиноятчиликнинг таҳдиди ва ундан ҳимояланиш усулларига тўхталишдан олдин, қуйидаги тушунчаларга таъриф бериб ўтиш мақсадга мувофиқдир:

[19] Кибержиноятчиликка қарши қандай курашиш керак? **Қутбиддин Бурханов, Олий Мажлис Сенати Мудофаа ва хавфсизлик масалалари қўмитаси раиси. 2020 йил 2 декабрь.**

кибержиноятчилик — ахборотни эгаллаш, уни ўзгартириш, йўқ қилиш ёки ахборот тизимлари ва ресурсларини ишдан чиқариш мақсадида кибермаконда дастурий таъминот ва техник воситалардан фойдаланилган ҳолда амалга ошириладиган жиноятлар йиғиндиси;

кибермакон — ахборот технологиялари ёрдамида яратилган виртуал муҳит;

кибертаҳдид — кибермаконда шахс, жамият ва давлат манфаатларига таҳдид солувчи шарт-шароитлар ва омиллар мажмуи;

киберхавфсизлик — кибермаконда шахс, жамият ва давлат манфаатларининг ташқи ва ички таҳдидлардан ҳимояланганлик ҳолати;

киберҳимоя — киберхавфсизлик ҳодисаларининг олдини олишга, киберҳужумларни аниқлашга ва улардан ҳимоя қилишга, киберҳужумларнинг оқибатларини бартараф этишга, телекоммуникация тармоқлари, ахборот тизимлари ҳамда ресурслари фаолиятининг барқарорлигини ва ишончлилигини тиклашга қаратилган ҳуқуқий, ташкилий, молиявий-иқтисодий, муҳандислик-техник чора-тадбирлар, шунингдек маълумотларни криптографик ва техник жиҳатдан ҳимоя қилиш чора-тадбирлари мажмуи;

киберҳужум — кибермаконда аппарат, аппарат-дастурий ва дастурий воситалардан фойдаланган ҳолда қасддан амалга ошириладиган, киберхавфсизликка таҳдид соладиган ҳаракат[20].

Касперский лабораториясининг маълумот беришича, бугунги кунга келиб ҳар куни халқаро интернет тармоғида 310 мингдан зиёд зарарланган дастурий вируслар тарқатилмоқда. 2006 йилларда ушбу кўрсаткич 1,4 мингтани ташкил қилар эди. Бу эса халқаро интернет тармоғидаги киберҳужумлар диапазони ўтган ўн йил ичида камида 200 марта ошганидан далолат беради[21].

Хозирги пайтда вируслар орқали амалга оширилаётган киберҳужумлар жуда хатарли тус олмоқда. Тарқатилаётган вирусларнинг аксарияти банк хизматларини кўрсатадиган жаҳон ахборот тармоғини заифлаштириш орқали, у ердан молиявий маълумотларни ўғирлашни кўзлайдилар.

2023 йил таҳлилларидан маълум бўлишича, банк-молия соҳасидаги йирик муассасалар, онлайн тўлов жараёнларини амалга оширувчи тизимлар, савдо мажмуалари, меҳмонхона ва савдо терминаллари энг кўп фойдаланиладиган марказлар хакерларнинг асосий диққат марказида туради.

Мисол учун, Carbanak кибер жиноятчилик гуруҳи ҳамда унинг SWIFT номли хакерлари банк ва бир қатор молиявий институтлардан ҳар йили 1 млн АҚШ долларидан зиёд маблағни ўғирлайдилар. Бу турдаги жиноятларни амалга ошириш катта маблағ келтиргани ҳамда бу жиноятларни фош этиш қийин бўлгани сабабли ҳам, бугун хакерлик жиноятлари ва шунга ўхшаш ахборот хуружлари сони ортиб бормоқдалар[22].

---

[20] Ўзбекистон Республикасининг 2022 йил 15 апрелдаги “ Киберхавфсизлик тўғрисида”ги ЎРҚ-764-сон Қонуни.

[21] https://ictnews.uz/uz/09/08/2017/kiber-jinoyatchilik/

[22]

Охирги йилларда молиявий ўғирликни кўзлаган фишинг ҳужумлари сон ва профессионаллик жиҳатдан ошган. Хусусан, хакерларнинг «кўринмас қармоғи»орқали ахборот хуружларини уюштириши ошиб, жами молиявий кибер ҳужумларни кўзлаган хакерлик жиноятларининг фоизи ошиб бормоқда. Жумладан, одамларга банк хизматларини кўрсатишни таклиф қилиш, сохта банк тизимларини яратиш орқали зарур ахборотларни ўғирлаш, электрон почталар орқали банк тизимларига ҳужум уюштириш, интернет тармоғида турли хилдаги қизиқарли акция ва викториналарни ташкил этиш орқали фойдаланувчиларнинг маълумотларини ўғирлаш ҳолатлари кузатилмоқда.

Сунги йилларда банк тизимларини ишдан чиқаришни мақсад қилган «троян»вируслари сони ошиб бормоқда. Улар орасида айниқса «Zbot»энг кўп тарқалган, «Gozi», «Nymaim», «Shiotob»оммалашаётган зарарли файллар оиласи. Бундай вирус ҳужумига учраган одамларнинг 17.17 фоизи тизимлардан корпоратив шаклда фойдаланувчилар бўлишган. Бундай зарарли файлларни тарқалиши асосан Россия, Германия, Япония, Вьетнам ҳамда АҚШда кўп кузатилган. Бугун бу каби вируслар туфайли молиявий зарар кўраётган кичик фирмалар сони ҳам ортиб бормоқда.

Android тизими фойдаланувчиларига уюштирилган ҳужумлари сони сунги йилларда 430 фоизга ошиб, жаҳон миқёсида 305,000 тани ташкил қилмоқда. Жумладан, Россия, Австралия, Украина давлатларида бу вирусларнинг кенг тарқалгани маълум бўлган.

Хусусан, Россия ҳудудида «Asacub»ҳамда «Svpeng»номли вируслар оиласи оммалашган. Бу вируслар жамланмаси маълум бир сайт эгаси Google сайтига реклама қўйишга рухсат бериши эвазига ундан пул олиши мумкин бўлган Google AdSense хизмати орқали тарқалган. Бунда Google рекламаси мавжуд сайтга кирган Android фойдаланувчиси зарарли файлни юқтириб олади ва хакерларнинг «қурбони»га айланадилар[23].

Шу боис, ахборот хавфсизлиги соҳаси мутахассислари Android операцион тизимида фаолият кўрсатувчи девайслар эгаларига интернетдан фойдаланишда ишончли манбааларга киришни маслаҳат бермоқдалар. Айниқса, банк-молиявий иловалари ўрнатилган мобиль қурилмаларга зарарли иловаларни ортириб олиш катта йўқотишларга сабаб бўлиши мумкин.

Кучли рақобат – хакерлик ривожига хизмат қилмоқдалар. Сўнгги йилларда хакерларнинг веб-сайтларга уюштираётган ҳужумлари сони тобора ошиб бормоқда. Ўтган асрнинг 60-йилларида «хакер»сўзи компьютер ва ахборот технологияларини пухта билган инсонларга нисбатан ишлатилган. Бугунги

Мисол учун, Carbanak кибер жиноятчилик гуруҳи ҳамда унинг SWIFT номли хакерлари банк ва бир қатор молиявий институтлардан ҳар йили 1 млн АҚШ долларидан зиёд маблағни ўғирлайдилар. Бу турдаги жиноятларни амалга ошириш катта маблағ келтиргани ҳамда бу жиноятларни фош этиш қийин бўлгани сабабли ҳам, бугун хакерлик жиноятлари ва шунга ўхшаш ахборот хуружлари сони ортиб бормоқдалар.

[23] https://ictnews.uz/uz/09/08/2017/kiber-jinoyatchilik/

кунга келиб эса бу сўз ахборот-коммуникация технологиялари ёрдамида ноқонуний ҳаракатларни бажарувчи, ахборот тизимлари ва дастурларини бузиб кириб, улардан рухсатсиз фойдаланувчи, илова ҳамда веб-саҳифалар муҳофазасини бузиш ва вирус тарқатиш орқали кибер жиноятчилик уюштирадиган шахсга нисбатан ишлатилади.

АҚШнинг Arbor Networks дастурий таъминот ишлаб чиқарувчи компанияси томонидан ўтказилган тадқиқот натижалари маълум қилишича, ишлаб чиқариш, компаниялар ўртасидаги рақобатнинг кучайиши уларни виртуал дунёда ҳам рақибга айлантирган ва компаниялар рақибларининг онлайн савдоси ёки тизимларини ишдан чиқариш мақсадида, хакерларни ёлламоқдалар.

Замонавий кибержиноятчилик орқали бугун хакерлар уларни ёллаётган муассасаларга хизматларини сотишга муваффақ бўлмоқдалар. Улар ўзлари кирган тизимлардан маълумотларни ўғирлаб, мижозларига сотадилар. Ёки ёлланма қотиллар каби, бошқа компаниянинг ахборот тизимларини йўқ қиладилар.

Ушбу хизматлари учун хаккерларга соатига 2.50 АҚШ доллари миқдорида иш ҳақи тўланар экан. Айниқса, бир нечта компьютерлар тармоғида хизмат кўрсатишни рад қилувчи зарарли тизимларнинг ўрнатилиши, яъни DDoS-ҳужумларга эҳтиёж ортиб бормоқдалар.

Тахминан ҳар йили 15 млн нафар АҚШ фуқароларига, асосан компания раҳбарларига оид 50 млн АҚШ доллари миқдоридаги зарарга тенг бўлган шахсий маълумотлар интернет тармоғига уюштирилган ҳужумлар оқибатида ўғирланадилар. Таҳлиллар бу каби жиноятларнинг асосан дам олиш кунларида содир бўлишини кўрсатади.

Arbor Networks таҳлилчиси Деннис Шварцнинг маълум қилишича, хакерларнинг соатига 2-3 АҚШ доллари ишлашлари кутилмаган ҳолат. Боиси, ривожланган мамлакатларда хакерлик учун жиноятчилар қатъий жазога тортиладилар. Уларнинг арзимаган маблағ эвазига жиноятга қўл уришлари эса ачинарли холатдир.

2017 йилнинг 7 февраль куни Москва шаҳрида бўлиб ўтган Кибер хавфсизлик бўйича халқаро форум (Cyber Security Forum-2017)да кибер жиноятлар оламида бугун энг кўп тарқалган учта хуруж қайд этилган[24].

Экспертларнинг фикрича, фишинг орқали маълумотларни ўғирлаш, махфий мақсадга эга мобиль иловалар орқали электрон қурилмаларга кириб бориш ва алоқанинг ҳимоя қилинмаган каналларини томоша қилиш орқали бугун кўпчилик интернет фойдаланувчилари кибер жиноятларнинг қурбонига айланмоқдалар.

Бугунги кунда кибер жиноятчиликда муайян шахснинг ёки объектнинг географик жойлашган нуқтаси тўғрисида хабар тарқатиш, шахсий маълумотлар базасини бузиб кириш каби хизматлар оммалашган. Хаккерлар бу каби маълумотларни интернет ва ижтимоий тармоқ фойдаланувчилари томонидан

[24]https://uza.uz/uz/posts/kiber-zhinoyat-tekhnologiya-yutu-larini-arazli-ma-sadlarga-y-04-08-2020?ysclid=m3tqt4qzpa720317103

турли электрон ресурсларга уларнинг фойдаланиш шартларини ўқимасдан туриб киришлари эвазига олишмоқда.

Яъни, биз ижтимоий тармоқда дуч келадиган “Неча йил яшайсиз?”, “АҚШ президенти сиз ҳақингизда нима дейди?”, “Қайси Голливуд актёрига ўхшайсиз” каби хизматлар аслида фишинг бўлиб, сиз улардан фойдаланиш чоғида уларнинг шартига рози бўласиз ва ўзингиз тўғрингиздаги маълумотларни уларга ҳадя қилган бўласиз. Бу маълумотлар эса махфий равишда ташкил этилган йирик “қора ахборот бозорлари”да катта маблағга сотиладилар.

“Касперский лабораторияси” асосчиси ва раҳбари Евгений Касперский 2017 йилнинг 27 февралидан 2 мартга қадар Барселонада ўттган Mobile World Congress анжумани чоғида замонавий техника, жумладан, интернетга уланган автомобиль ва уйларнинг хавфсизлиги билан боғлиқ муаммоларга тўхталиб ўтган[25].

Евгений Касперскийнинг таъкидлашича, сўнгги ойларда «ақлли уй»ва интернет буюмлар тизимларига уюштирилган йирик хуружлар аниқланган. Интернетга уланган ҳар қандай гаджетнинг IP-манзили орқали “ақлли уй”ларнинг ҳолати тўғрисида маълумотларни ўғирлаш, компьютерлар тармоғи бўлган ботнетларга ҳужум уюштириш мумкин.

Хакерлар нафақат видеокамералар, автомобиль, самолёт компьютерлари, балки бугун оммалашётган “ақлли чироқ”ларни, бундан ҳам жиддийроқ хавфсизлик тизимларини масофадан туриб ишдан чиқаришади ва уларнинг устидан назоратни қўлга олишадилар. Натижада, улар йирик авария, ёнғин ва бошқа турдаги бахтсиз ҳодисаларни сунъий равишда келтириб чиқаришадилар. “Касперский лабораторияси” тадқиқтоларидан маълум бўлдики, интернетга уланган деярли барча автомобилларнинг рақамли калитларини тайёрлаш ва тизимларини масофадан бошқариш мумкин экан.

Хакерлар 2016 йилда Украина ва Германиядаги йирик электростанцияларни вирус ёрдамида ўчириб қўйишлари билан боғлиқ хуружлар хакерларнинг атом станцияларига ҳам уюштириши мумкинлиги, бу эса фожеали техноген ҳалокатларни келтириб чиқаришидан далолат берадилар[26].

Евгений Касперский хакерларнинг хуружини инобатга олган ҳолда, янги кучли платформа яратиш ғоясини илгари сурган. Унинг сўзларига кўра, тўлиқ ҳимояланган тизимни яратиш иложсиз, бироқ замонавий хуружларга мослаша оладиган турли қурилмалар учун универсал ҳимоя тизимини яратишнинг имкони борлигини айтиб ўтган.

“Касперский лабораторияси” хакерлардан ҳимоя тизимларини ишлаб чиқиш бўйича тажрибали мутахассисларни ишга олади. Касперский ҳар қандай тизимни ишлаб чиқишда, аввало, унинг хакерлик хуружларига чидамлилигини ҳисобга олиш кераклигини айтдилар.

Яна бир қизиқарли далил – Евгений Касперский смартфондан фойдаланмайдилар. Унинг Жаҳон Мобиль Конгресси чоғидаги чиқишида тадбир бошловчиси ундан мобиль алоқа воситасини кўрсатишини сўраганида

[25] http://ran-nauka.ru/wp-content/uploads/2014/09/Nauka-1-2019.pdf

[26] https://cyberleninka.ru/article/n/internet-or-ali-sodir-etiladigan-firibgarlik-zhinoyatlari-horizh-tazhribasi?ysclid=m3tqylqczt47137732

Касперский Sony Ericsson брендидаги эски телефонни қўлига олди. Унинг сўзларига кўра, эски телефондан фойдаланиш унинг учун қулай, бу унга ҳеч қачон панд бермайди. Энг муҳими, у замонавий смартфонлар каби нозик эмас.

“Касперский лабораторияси”нинг гувоҳлик беришича, Ўзбекистон Республикасида кибер хуружга учраётганларнинг 1,6 фоизига банк-троянлари зарар етказмоқдалар. Кибер-вирус хуружига учраганлар орасидан банк-троянларининг қурбонига айланган фойдаланувчилар улуши бўйича Ўзбекистон Республикаси жаҳондаги энг юқори кўрсаткичга эга 10 та мамлакат қаторида 10-ўринни эгаллаган. Мобиль қурилмалар хавф-хатари географиясига мувофиқ, Ўзбекистон Республикасидаги мобиль қурилмаларга йилида 1000 тадан 50 мингтагача зарарли вирусга эга иловалар зарар етказадилар.

Бугун тадбиркорлик соҳаси ривожланаётган, олди-сотди муносабатлари рақамли тизимларга кўчаётган бир пайтда ахборот хавфсизлигини таъминлаш масаласининг аҳамияти ҳам ошиб бормоқдалар. Verizon Data Breach Report таҳлилида ёзилишича, барча кибер хуружларнинг 71 фоизи камида 100 нафар ходим ишлайдиган катта компанияларга уюштириладилар. Бу ҳужумлар муваффақиятли якун топса, “жабрланувчи” муассаса камида 36 000 АҚШ доллари зарар кўрадилар.

Компьютер тизимларига киришга рухсат берувчи паролларни ҳар 6 ойда бир марта янгилаш зарурлигини жаҳонинг аксарият компаниялари одатларига айлантиришган. Аксарият хакерлар умумий пароллар билан ҳужум уюштирадилар.

Шуни алоҳида таъкидлаш жоизки, ходим – хавфсизликнинг энг нозик нуқтаси. Фишинг-ҳужумлар фойдаланувчининг электрон почтаси, ижтимоий тармоғидаги саҳифалари орқали ахборотларни ўғирлашга уринишади. Хакер логин ва махфий сўзларни аниқлашга уриниб, ходимларга сохта, аслига айнан ўхшаш сайтларнинг манзилини юборади. Бу кибер жиноятчиликнинг олдини олиш учун эса ходим малака ва билимга муҳтож.

Махфий маълумотларнинг хакерлар қўлига тушиш ҳолати кўпроқ собиқ ходимлар билан боғланадилар. Шунингдек, заиф веб-сайтлар, айниқса онлайн тўлов ҳамда тизимлар ўрнатилган сайтларда кучли ҳимоялаш чораларини кўриш зарур.

Муҳим информация доимо шифрланган шаклда сақланиши лозим. Яъни, маълумотларни шифрлаш тизимларини ўрнатиш мақсадга мувофиқ.

Мутахассисларнинг фикрича, агар ҳар бир интернет фойдаланувчиси ва хизмат кўрсатувчилар кибер оламда ҳам ҳаётдаги каби эҳтиётқорликни унутмасалар, аксарият кибер жиноятларнинг олди олинган бўлар эдилар.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Ўзбекистон Республикасининг Конституцияси. – Т., 2023й.
2. Мирзиёев Ш.М. Миллий тараққиёт йўлимизни қатъият билан давом эттириб, янги босқичга кўтарамиз. – Тошкент: “Ўзбекистон”, И жилд. НМИУ, 2017, – 592 б.
3. Ўзбекистон Республикасининг 2022 йил 15 апрелдаги “ Киберхавфсизлик тўғрисида”ги ЎРҚ-764-сон Қонуни.

4. Кибержиноятчиликка қарши қандай курашиш керак? Қутбиддин Бурханов, Олий Мажлис Сенати Мудофаа ва хавфсизлик масалалари қўмитаси раиси. 2020 йил 2 декабрь.
5. https://ictnews.uz/uz/09/08/2017/kiber-jinoyatchilik/
6. [1]https://uza.uz/uz/posts/kiber-zhinoyat-tekhnologiya-yutu-larini-arazli-ma-sadlarga-y-04-08-2020?ysclid=m3tqt4qzpa720317103.
7. https://cyberleninka.ru/article/n/internet-or-ali-sodir-etiladigan-firibgarlik-zhinoyatlari-horizh-tazhribasi?ysclid=m3tqylqczt47137732.
8. ttp://ran-nauka.ru/wp-content/uploads/2014/09/Nauka-1-2019.pdf

KIBERJINOYATCHILIK VA INTERNET TARMOQLARINING YOSHLAR TARBIYASIGA SALBIY TA'SIRI

Otayev O'tkirbek Matyoqubovich

O'zbekiston Respublikasi IIV Malaka oshirish instituti Kasbiy tayyorgarlik fakulteti Maxsus fanlar sikli katta o'qituvchisi
Tel:+99897 775 08 83

Annotasiya: Mazkur maqolada «Kiberjinoyatchilik» tushunchasi, axborot-kommunikasiya texnologiyalari vositalari va internet tarmoqlarining yoshlar tarbiyasiga salbiy ta'siriga ilmiy asoslangan ma'lumotlar berilgan.

Kalit so'zlar: Kiberjinoyatchilik**,** internet**,** yoshlar, axborot huruji, jinoyat, kiberhujum, halqaro tajriba.

Аннотация: В статье представлена научно обоснованная информация о понятии «Киберпреступность», негативном влиянии информационно-коммуникационных технологий и Интернета на образование молодежи.

Ключевые слова: Киберпреступность, Интернет, молодежь, информационная атака, преступность, кибератака, международный опыт.

Abstract: This article provides scientifically based information on the concept of "Cybercrime", the negative impact of information and communication technologies and Internet networks on the upbringing of young people.

Keywords: Cybercrime, Internet, youth, information attack, crime, cyberattack, international experience.

XXI asr – axborot texnologiyalari taraqqiyoti asri. Bugungi kun taraqqiyotini jahon axborot tarmog'i internetsiz tasavvur qilish mushkul. Ma'lumki, internet axborot va hujjatlarning o'zaro almashinishini ta'minlaydigan kompyuter tarmoqlarini birlashtirgan xalqaro tizimdir. Internet keng imkoniyatlar eshigini ochdi. Uydan ko'chaga chiqmay turib global tarmoq orqali dunyo kutubxonalari bo'ylab sayr qilish, kurrai zaminning narigi chekkasida joylashgan oliy ta'lim muassasasining masofaviy (virtual) talabasi bo'lish, hatto elektron xizmatlarni (matnlarni tarjima qilish, video va audiomahsulotlarni tayyorlab berish, kitob va risolalarni sahifalash va hokazo) shartnoma orqali bajarish, pul ishlab topish mumkin. Xullas, internetning ijobiy jihatlari bisyor. Ijtimoiy tarmoqlar yoki messenjerlarning qulayligichi? Onlayn konferensiyalar o'tkazish, onlayn malaka oshirish, yaqinlar va tanish bilishlar bilan tez,

arzon video yoki audiomuloqot qilish. Mana shu jihatlari bilan internet keyingi paytlarda jozibadorlikda televideniye, radio va boshqa axborot vositalarini ortda qoldirmoqda. Lekin internet ko‘plab foydali jihatlari bilan birga salbiy oqibatlarini ham namoyon qilmoqda. Ayniqsa, yoshlarda axborot iste’moli madaniyatining sustligi, turli xabarlar oqimidan kerakligini ajratib olishda bilim, malaka va ko‘nikmaning yetishmasligi ba’zilarning g‘arazli kimsa va oqimlar ta’siriga tushib qolishlariga, internet qaramligi kasalligiga yo‘liqishlariga sabab bo‘lmoqda. Xitoy Xalq Respublikasida internetga qaramlik kasallik sifatida e’tirof etilib, uni davolovchi maxsus shifoxonalar tashkil etilgani so‘zimizning isbotidir.

Aksariyat yoshlar o‘zlarining qimmatli vaqtlarini behuda sarflab, ijtimoiy tarmoqlardan kun bo‘yi foydalanishadi. Shu tariqa, ular deyarli barcha axborotga ega bo‘lishadi va o‘z dunyoqarashidan kelib chiqib, u yoki bu masalaga munosabat bildirishadi. Biroq bildirilgan munosabatlarning barchasini saviyali, ya’ni ma’naviyatli kishilarning fikri, deb bo‘lmaydi, albatta. Ayniqsa, bugungi kunda yetarli bilim va ko‘nikmalarga ega bo‘lmagan kimsalar ham to‘g‘ri yo noto‘g‘riligini o‘ylab o‘tirmasdan, ijtimoiy tarmoqlarda tarqatilgan har qanday ma’lumot yuzasidan yoxud ba’zi masalalarga bilim va salohiyati yetadimi, yo‘qmi, bundan qat’i nazar, o‘z fikrini bildirishadi. Yoki o‘zlarining yozgan «asarlari» yo »maqola», «xabar», «she’r»larini ijtimoiy tarmoqlarga joylashtirib, bir-birlarini ko‘klarga ko‘tarib maqtashadi. Qizig‘i shundaki, ba’zi odamlar aslida shu ishni qilish kerakmi, yo‘qmi, degan ishtibohga ham bormaydi. Ijtimoiy tarmoqlarda havola etiladigan ma’lumotlarni «bezab turgan» g‘aliz jumlalar hamda imloviy xatolar o‘sha tarmoq foydalanuvchisining saviyasi qay darajada ekanligini ko‘rsatib turadi. Bu esa ijtimoiy tarmoq foydalanuvchilarida ham afsuslanish, achinish holatlarini keltirib chiqaradi. Ba’zida esa ijtimoiy tarmoqlar orqali havola etilayotgan asossiz va saviyasiz ma’lumotlarning sanab adog‘iga ham yetib bo‘lmaydi. Ayniqsa, tarmoqlarda shunday guruhlar ham paydo bo‘lganki, foydalanuvchilar bir-birini maqtab ko‘kka ko‘tarishlari, shuningdek, kimlarningdir nomini loyga chaplashlari oddiy holga aylanib bormoqda. G‘iybat ular uchun oddiy holga aylangan. Ba’zi kimsalar esa ijtimoiy tarmoqdan o‘zlariga yoqmagan odamlarning obro‘sini to‘kish, yerga urish, buning uchun bor imkoniyatidan foydalanishga harakat qilishadi. Ijtimoiy tarmoqlarni nazoratga olish imkoniyati yo‘qligi bois, unda har qanday ishni qilish mumkin, deb o‘ylashadi. Erkin fikr aytish imkoniyatidan shunday yo‘llar bilan foydalanish mumkin deganlar, saviyalari qay darajada ekanliklarini katta auditoriyaga shunday yo‘llar bilan oshkor qilishadi. Shu sabab ko‘pchilik bu tarmoqlarni yoqtirishmaydi. Lekin shunga qaramay, statistik ma’lumotlarga nazar solsak, dunyo yoshlarining 96 foizi ijtimoiy tarmoqlar vositasida o‘zaro muloqotga kirishishmoqda. Olib borilgan axborot-tahliliy natijalar va statistik ma’lumotlarga ko‘ra, Facebook hozirgi vaqtda dunyoda eng mashhur ijtimoiy tarmoq sifatida yetakchi o‘rinda bormoqda. Bugungi kunga kelib, Facebook tarmog‘ida ro‘yxatdan o‘tganlar soni bir necha milliard kishidan ortganligi ma’lum qilingan. Undan keyingi o‘rinlarni esa Twitter, Instagram, LinkedIn, Google+, Pinterest, Snapchat, YouTube, Reddit, WhatsApp, Flickr, Weibo egallab kelmoqda. Bugungi kunda ijtimoiy tarmoqlarda mamlakatimizda amalga oshirilayotgan islohotlar, davlatimiz qo‘lga kiritayotgan olamshumul yutuqlarni jahon media makonida keng

targ‘ib qilish hamda inson ma’naviyatini har tomonlama yuksaltirishga xizmat qiladigan juda ko‘plab ma’lumotlar yoritib borilmoqda.

Asrimizning global muammolari qatoriga yangidan-yangi turlari bilan tilga olinayotgan kiberjinoyatchilik kirib kelganiga ham ancha bo‘ldi. Uning bizga ma’lum bo‘lgan virusli dasturlarni tarqatish, parollarni buzib kirish, kredit karta va boshqa bank rekvizitlaridagi mablag‘larni o‘zlashtirish talon-toroj qilish, shuningdek, internet orqali qonunga zid axborotlar, xususan, bo‘hton, ma’naviy buzuq ma’lumotlarni tarqatish bilan bashariyat hayotiga katta xavf solayotganidan ko‘z yuma olmaymiz. «Kiberjinoyatchilik» tushunchasi axborot-kommunikasiya texnologiyalari vositalaridan foydalangan holda, virtual tarmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish (spam), xakerlik hujumi, vebsaytlarga noqonuniy kirish, firibgarlik, ma’lumotlar butunligi va mualliflik huquqini buzish, kredit kartochkalari raqami hamda bank rekvizitlarini o‘g‘irlash (fishing va farming) va boshqa turli huquqbuzarliklar bilan izohlanadi. Shu o‘rinda kiberterrorizm va uning jamiyat hayotiga solayotgan xavfining ko‘lami ham oshib borayotganini ta’kidlash joiz. Kiberterroristik harakat (kiberhujum) – kompyuterlar va axborot kommunikasiya vositalari yordamida amalga oshirilgan, odamlarning hayoti va sog‘lig‘iga bevosita xavf tug‘diradigan yoki potensial xavf tug‘dirishi mumkin bo‘lgan, moddiy obyektlarga katta zarar yetkazishi yoki shunga olib kelishi mumkin bo‘lgan, ijtimoiy xavfli oqibatlarning boshlanishi yoki maqsadi bo‘lgan siyosiy sababdir. Zamonaviy terrorchilar uchun kibermakondan foydalanishning jozibadorligi kiberhujumni amalga oshirish katta moliyaviy xarajatlarni talab qilmasligi bilan bog‘liq.

Ekspertlarning xulosasiga ko‘ra, bu rivojlanayotgan davlatlarning taraqqiyotiga ko‘maklashish, umuminsoniy demokratik tamoyillarni qaror toptirish niqobi ostida fuqarolar ongiga ta’sir o‘tkazish, ularni turli yo‘llar bilan o‘z maqsadlari sari bo‘ysundirish orqali amalga oshirilmoqda. Afsuski, bu jarayonda kiberhujumlarni uyushtirish, bu yo‘lda internet global tarmog‘ining mislsiz imkoniyatlaridan «samarali» foydalanishga urinishlar tobora avj olmoqda. Internetda mavjud ijtimoiy tarmoqlar, ularning ishlab chiqaruvchilari va homiylarining suveren davlat ichki ishlariga «aralashish-lari» qanday rol o‘ynashi oxirigacha o‘rganilmaganligi bois ba’zan bunday «aralashuv» mazkur davlatga qarshi ekanligi hali hanuz e’tirof etilgani yo‘q. Internet saytlari to‘satdan paydo bo‘lib, ko‘pincha formatini, so‘ngra manzilini o‘zgartiradi. Shu bois ayrim ekspertlar internetning butkul ochiqligi kabi dastlabki konsepsiyalardan voz kechib, uning yangi tizimiga o‘tishni taklif etmoqda. Yangi modelning asosiy mohiyati tarmoqdan foydalanuvchilarning anonimligidan voz kechishdir. Bu tarmoqning jinoiy tajovuzlardan yanada ko‘proq himoyalangan bo‘lishini ta’minlashga imkon berdi. Misol tariqasida, yopiq tarmoq tizimiga o‘tgan Xitoy davlatini va bunday jarayonga tayyorgarlik ko‘rayotgan Rossiya davlatini keltirishimiz mumkin.

Jahon hamjamiyatiga integrasiyalashayotgan mamlakatimizda axborot kommunikasiya texnologiyalari, axborot tizimlari va zamonaviy kompyuter texnologiyalaridan samarali foydalanish bo‘yicha izchil davlat siyosati olib borilmoqda. Bugungi kunda mamlakatimizda joriy etilayotgan zamonaviy raqamli texnologiyalar, fuqarolarimizga qator qulayliklar va imkoniyatlar eshigini ochmoqda.

Mazkur jarayon bilan bir qatorda, yaratilayotgan raqamli texnologiyalar va axborot tizimlarining xavfsizligini ta’minlash muammosi ham mavjud, albatta. Bu eng dolzarb masalalardan biri kiberxavfsizlikni ta’minlash, sodir etilishi mumkin bo‘lgan kiberjinoyatlarning oldini olish va unga qarshi kurashish masalasi hisoblanadi.

Kundan-kunga takomillashib ketayotgan kiberjinoyatchilikka qarshi kiberxavfsizlikni ta’minlashda quyidagi asosiy talablarni bajarish orqali ulardan himoyalanish, ya’ni kiberxavfsizlikni ta’minlashimiz mumkin:

– xodimlarga axborot xavfsizligi asoslarini o‘rgatish;
– foydalanayotgan dasturiy mahsulotlarning zaifliklarini doimiy sinovdan o‘tkazish;
– ishonchli antivirus dasturidan foydalanish;
– lisenziyalangan rasmiy dasturlardan foydalanish;
– axborot tizimlarini himoyalashda ko‘p faktorli autentifikasiyadan foydalanish;
– parollardan foydalanishda kuchli parolni saqlash siyosatiga rioya qilish;
– muntazam ravishda kompyuter qattiq disk-laridagi ma’lumotlarni shifrlash.

Shu o‘rinda, mamlakatimizda kiberjinoyatlarning oldini olish va unga qarshi kurashni olib boruvchi vakolatli davlat idoralariga ham muayyan vazifalar yuklanishini alohida ta’kidlash lozim. Xususan, ular kiberjinoyatchilikka qarshi kurash faoliyatida O‘zbekiston Respublikasi va uning xalqini axborot texnologiyalari va kommunikasiyalari orqali amalga oshirilayotgan yoki bunga imkon berayotgan shaxs, jamiyat va davlat xavfsizligini va ularning manfaatlari tashqi hamda ichki kibertahdidlardan himoya qilinishini ta’minlash, mazkur sohada qonuniylik va qonun ustuvorligini mustahkamlash, kiberjinoyatlar va kiberhuquqbuzarliklarning oldini olish, ularni aniqlash va barham berish kabi vazifalarni amalga oshirishi darkor.

Xulosa qilib aytganda, davlatimiz rahbari Shavkat Mirziyoyev ta’kidlaganidek, «... biz farzandlarimizning ongi, dunyoqarashi asrlar davomida sinovdan o‘tgan, yuksak ma’naviyat xazinasi bo‘lgan jahon va milliy adabiyotimiz asosida emas, balki qandaydir shubhali, zararli axborotlar asosida shakllanishiga beparvo qarab turolmaymiz». Binobarin, bugungi davr bizdan dunyo miqyosida bo‘hton va uydirmalarni tarqatish orqali yoshlarimizni aldab, o‘z qarmog‘iga ilintirishga intilayotgan ijtimoiy tarmoqlardagi turli salbiy holatlarga hyech qanday imkon bermasligimizni talab etmoqda. Zero, milliy ma’naviyatimizni asrash orqali yoshlarimizni ona Vatanga sadoqat ruhida tarbiyalab, o‘z xalqiga, yurtiga bo‘lgan muhabbatini oshirish asosiy vazifamizdir. Shuningdek, kiberjinoyatlar va kiberhuquqbuzarliklarni tergov qilish va ularni aniqlash, bartaraf etish hamda oldini olish bo‘yicha zarur qarorlar qabul qilish, kiberjinoyatchilikka qarshi kurashish bo‘yicha normativ-huquqiy hujjatlar loyihalarini ishlab chiqishda ishtirok etish, kiberterrorizm, kiberekstremizm, uyushgan jinoyatchilikka qarshi kurashish, davlat organlari manfaatlariga hamda kiberxavfsizligiga tahdid soluvchi kiberxatarlarni aniqlash va ularga qarshi kurashish, kiberjinoyatlar bo‘yicha tergovga qadar tekshiruv va dastlabki tergovni o‘tkazish, tezkor-qidiruv faoliyatini amalga oshirish, fuqarolarning huquq va erkinliklariga tahdid soluvchi kiberjinoyatlarning sodir etilishiga imkon yaratuvchi sabablar hamda shart-sharoitlarni aniqlash va bartaraf etish kabi muhim vazifalarni bajarishlari lozim

Foydalanilgan adabiyotlar

1. O‘.M.Otayev. Kiberhujum nima va u qanday sodir bo'ladi? Jamoat xavfsizligi universitetida Jinoyatchilikka qarshi kurashishda raqamli texnologiyalardan foydalanish mavzusidagi ilmiy-amaliy konferensiya materiallari. 18.06.2024 y.
2. O‘.M.Otayev Kibermakonda sodir etilayotgan xuquqbuzarliklar. IIV Akademiyasida. “Kiberxavfsizlikni ta’minlash va axborot texnologiyalari soxasidagi jinoyatlarga qarshi kurashishni takomillashtirish istiqbollari”.Respublika ilmiy-amaliy konferensiya to‘plami. 22.12.2023 y
3. A.Iminov. Kiberjinoyatchilikka qarshi – Kiberxavfsizlik 30.12.2020 yil.
4. M.Musaev. Ijtimoiy tarmoq: undan siz qanday foydalanasiz? 15.11.2020 y
5. Axborot Xurujlari: maqsad va shakllari Postda gazetasi 03.12.2018 yil

ЁШЛАР ОРАСИДА КИБЕРЖИНОЯТЧИЛИКНИНГ ОЛДИНИ ОЛИШГА ҚАРАТИЛГАН ТАРҒИБОТ ИШЛАРИ

Усманов Алишер Шарафиддинович

Ўзбекистон Республикаси Ички ишлар вазирлиги Малака ошириш институти Жисмоний тайёргарлик цикли бошлиғи

Аннотация: Мақолада ёшлар орасида кибержиноятчиликнинг олдини олишга қаратилган тарғибот ишларининг аҳамияти ва уларни амалга ошириш усуллари таҳлил қилинган. Кибержиноятчиликнинг ёшлар ҳаётига таъсири, интернет хавфларининг олдини олишда ахборот хабардорлигини ошириш, онлайн хулқ-атворни шакллантириш ва қонуний саводхонлик даражасини кўтариш каби масалалар ёритилган. Шунингдек, тарғибот ишларини самарали ташкил қилиш учун таълим муассасалари, оммавий ахборот воситалари ва ижтимоий тармоқларнинг ўрнига алоҳида эътибор қаратилган.

Калит сўзлар: Кибержиноятчилик, ёшлар, тарғибот ишлари, ахборот хавфсизлиги, интернет хавфлари, қонуний саводхонлик, ахборот маданияти, профилактика, ижтимоий тармоқлар, таълим.

ПРОПАГАНДА ПО ПРЕДУПРЕЖДЕНИЮ КИБЕРПРЕСТУПНОСТИ СРЕДИ МОЛОДЕЖИ

Усманов Алишер Шарафиддинович

Начальник цикла физической подготовки Институт повышения квалификации МВД Республики Узбекистан

Аннотация: В статье анализируется значение пропагандистской работы, направленной на предотвращение киберпреступности среди молодежи, и методы ее реализации. Освещены такие вопросы, как влияние киберпреступности на жизнь молодежи, повышение информационной осведомленности в предотвращении интернет-рисков, формирование онлайн-поведения и повышение уровня правовой грамотности. Также особое внимание уделяется

расположению образовательных учреждений, средств массовой информации и социальных сетей для эффективной организации пропаганды.

Ключевые слова: киберпреступность, молодежь, адвокация, информационная безопасность, интернет-риски, правовая грамотность, информационная культура, профилактика, социальные сети, образование.

ADVOCACY FOR THE PREVENTION OF CYBERCRIME AMONG YOUNG PEOPLE

Usmanov Alisher Sharafiddinovich

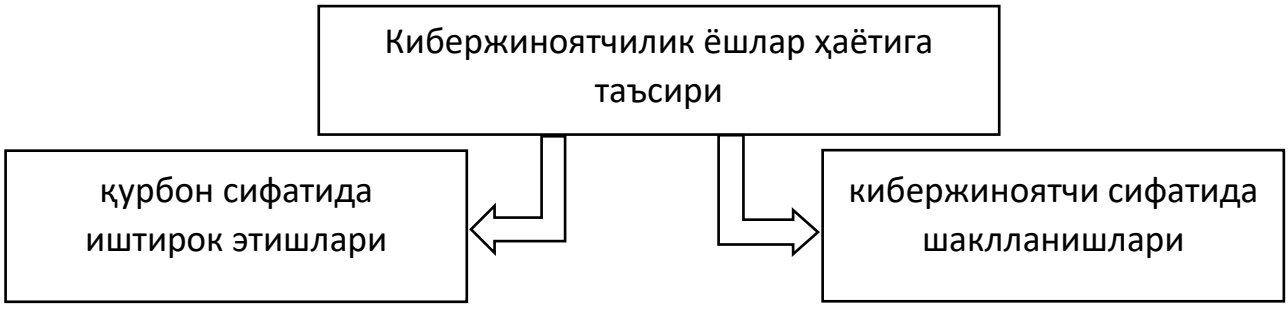
Head of physical training cycle Institute for Advanced Training of the Ministry of Internal Affairs of the Republic of Uzbekistan

Abstract: The article analyses the importance of advocacy work aimed at preventing cybercrime among young people and the methods of its implementation. Issues such as the impact of cybercrime on the lives of young people, raising information awareness in preventing Internet risks, shaping online behaviour and raising the level of legal literacy are highlighted. The location of educational institutions, media and social media for effective advocacy is also emphasised.

Keywords: cybercrime, youth, advocacy, information security, Internet risks, legal literacy, information culture, prevention, social media, education.

КИРИШ. Ҳозирги рақамли даврда интернет ва замонавий технологиялар ёшларнинг кундалик ҳаётининг муҳим қисмига айланган. Бу дунё ёшлар учун чекланмаган имкониятларни очиб берса-да, айрим хавфлар ҳам ўзи билан бирга келтирмоқда. Кибержиноятчилик бугунги кунда нафақат ёшлар орасида қурбонларнинг кўпайишига, балки уларнинг ўзлари кибержиноятчига айланиш ҳолатларининг ўсишига сабаб бўлмоқда. Бундай вазиятда киберхавфсизликни тарғиб қилишнинг аҳамияти ошиб бормоқда. Қуйида ушбу муаммони таҳлил қилиб, уни ҳал этиш йўллари муҳокама қилинади.

Кибержиноятчиликнинг ёшларга таъсири. Кибержиноятчилик ёшлар ҳаётига икки асосий йўналишда таъсир кўрсатади: улар қурбон сифатида иштирок этишлари ёки кибержиноятчи сифатида шаклланишлари мумкин.



1. Қурбонлар сифатидаги ёшлар:

- Шахсий маълумотларни ўғирлаш ёки улардан ноқонуний фойдаланиш ҳолатлари;

- Молиявий фирибгарликлар қурбони бўлиш орқали молиявий йўқотишларга учраш;

- Интернетда бузғунчи таъсирга учраб, ёшларнинг маънавий ёки руҳий зарар кўришлари.

2. Кибержиноятчи сифатидаги ёшлар:

- Зарарли дастурлар яратиш ва уларни тарқатиш;

- Бузғунчи ахборот хуружларида иштирок этиш;

- Бошқа шахсларнинг шахсий маълумотларини ноқонуний тарзда олиш ёки тарқатиш.

1-жадвал: Киберхавфларга қарши курашиш йўналишлари.

Кибержиноятчилик муаммолари	**Ёшларга таъсири**	**Ечимлар**
Шахсий маълумотларни ўғирлаш	Шахсий ёки молиявий маълумотларнинг ёйилиши хавфи	Ахборот хавфсизлиги қоидаларини ўргатиш, кучли пароллардан фойдаланишни тавсия қилиш
Онлайн фирибгарлик	Молиявий йўқотишларга учраш	Ёшларга фирибгарлик турлари ҳақида маълумот бериш, ҳимояланган тўлов тизимларидан фойдаланишни тушунтириш
Зарарли дастурлар тарқатиш	Ёшларнинг кибержиноятчига айланиш хавфи	Этик ҳулқ-атвор қоидаларини ўргатиш, қонунчилик оқибатларини тушунтириш
Бузғунчи ахборот хуружлари	Жамиятда ноқонуний маълумот тарқатиш билан боғлиқ муаммолар	Интернетда масъулиятли фойдаланиш маданиятини ривожлантириш
Бошқа шахсларнинг маълумотларига рухсатсиз кириш	Қонуний оқибатлар ва руҳий зарарга дуч келиши	Қонуний билимларни ошириш, ахборот хавфсизлигини таъминловчи дастурлардан фойдаланишни тавсия қилиш

Тарғибот ишларининг аҳамияти киберхавфларга қарши профилактика чоралари ёшлар онгида интернетдан тўғри фойдаланиш кўникмаларини шакллантиришга қаратилган бўлиши лозим. Бу йўналишда қуйидаги ишлар муҳим аҳамият касб этади:

1. Ахборот хабардорлигини ошириш:

- Интернет хавфлари ва уларнинг оқибатлари ҳақида маълумот тарқатиш.

- Ёшларни кибержиноятчиликнинг ҳуқуқий оқибатлари билан таништириш.

2. Онлайн хулқ-атворни шакллантириш:

- Интернетда масъулиятли ва этик хулқ-атвор қоидаларини ўргатиш.

- Ахборот хавфсизлиги маданиятини ривожлантириш.

3. Қонуний саводхонликни ошириш:

- Ёшлар орасида кибержиноятчилик турлари ҳақида тушунчалар бериш.

- Давлатнинг рақамли хавфсизликка оид сиёсати ҳақида маълумот тарқатиш.

Тарғибот ишларини амалга ошириш усуллари. Ёшлар орасида киберхавфсизликни тарғиб қилиш самарали усулларни талаб этади. Булардан айримлари қуйида келтирилган:

1. Таълим муассасаларида ўтказиладиган тадбирлар:

- Мактабларда ва университетларда киберхавфсизлик мавзусида семинарлар ташкил этиш.

- Ўқув дастурларига киберхавфсизлик бўйича махсус дарсларни киритиш.

2. Оммавий ахборот воситалари орқали тарғибот:

- Телевидение ва радио орқали киберхавфлар ҳақида маълумот тарқатиш.

- Интернет платформаларида ижтимоий реклама орқали киберхавфсизликни ёритиш.

3. Ижтимоий тармоқлардан фойдаланиш:

- Ижтимоий тармоқларда киберхавфсизликка бағишланган саҳифалар яратиш.

- Киберхавфсизлик мавзусида челленжлар ва флешмоблар ташкил этиш.

4. Ролли ўйинлар ва амалий машғулотлар:

- Киберхавфларни симуляция қилувчи ўйинлар ёрдамида ёшларнинг онгини ошириш.

- Амалий машғулотлар орқали киберхавфларга қарши ҳимоя стратегияларини ўргатиш.

Тарғибот ишларининг самарадорлигини ошириш. Киберхавфсизлик бўйича тарғибот ишларининг натижадорлигини ошириш учун кўплаб ресурслардан фойдаланиш талаб этилади:

1. Ҳамкорликни кенгайтириш:

- Давлат ва нодавлат ташкилотлар билан биргаликда дастурлар ишлаб чиқиш.

- Ёшлар ташкилотлари орқали киберхавфсизликни тарғиб қилиш.

2. Технологик имкониятлардан фойдаланиш:

- Киберхавфсизлик бўйича мобил иловалар яратиш ва улардан фойдаланишни рағбатлантириш.

- Интернет қурилмаларида хавфсизлик дастурларини жорий қилиш.

3. Раҳбарлик ва намуналар яратиш:

- Ёшларни киберхавфсизликка оид лойиҳаларда фаол иштирок этишга жалб этиш.

- Киберхавфларга қарши илғор ташаббусларни қўллаб-қувватлаш.

ХУЛОСА

Ёшлар орасида киберхавфсизлик маданиятини шакллантириш нафақат уларнинг шахсий хавфсизлигини таъминлаш, балки жамиятни киберхавфлардан ҳимоя қилишда ҳам катта аҳамиятга эга. Тарғибот ишлари ёшларни интернетда

масъулиятли хулқ-атворга ўргатиб, кибержиноятчиликка қарши курашишга ёрдам беради.

ТАВСИЯЛАР

1. Киберхавфсизлик соҳасида махсус дастурлар ишлаб чиқиш.
2. Интернет хавфсизлиги бўйича танловлар ва мусобақалар ташкил қилиш.

АДАБИЁТЛАР

1. Крымов А.А. К вопросу о направлениях деятельности по профилактике суицидального поведения в молодежной среде. // Человек: преступление и наказание, 2017.

2. Хомутов М.В., Грибанов Е.В. Основные направления, положительный опыт и проблемы совершенствования участия социально ориентированных некоммерческих организаций в специальной профилактике преступлений. // Общество и право, 2022.

3. Кобец П.Н. Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения. // Вестник Самарского юридического института, 2022.

4. Богданов А.В. Основные направления деятельности полиции по предупреждению и профилактике правонарушений среди несовершеннолетних. // Вестник Московского университета МВД России, 2017.

КИБЕРЖИНОЯТЧИЛИККА ҚАРШИ ПРОФИЛАКТИКАДА АХБОРОТ МАДАНИЯТИНИНГ АҲАМИЯТИ

Албеков Шокир Адилбекович

Ўзбекистон Республикаси Ички ишлар вазирлиги Малака ошириш институти Жисмоний тайёргарлик цикли катта ўқитувчиси

shokiralbekov@gmail.com

Аннотация: Ушбу мақолада кибержиноятчиликка қарши профилактикада ахборот маданиятининг аҳамияти таҳлил қилинган. Ахборот маданияти тушунчаси, унинг киберхавфларнинг олдини олишдаги роли ва самарадорлиги ёритилган. Шунингдек, ахборот маданиятини ривожлантириш учун таълим, тарғибот ва технологик ечимларнинг аҳамияти қайд этилган. Мақола ахборот хавфсизлигини таъминлашдаги инновацион ёндашувларни ҳамда жамиятда ахборот маданиятини шакллантириш йўлларини ўрганишга қаратилган.

Калит сўзлар: кибержиноятчилик, ахборот маданияти, ахборот хавфсизлиги, профилактика, рақамли саводхонлик, таълим, тарғибот, технологик ечимлар, киберхавфлар, жамоат хавфсизлиги.

ЗНАЧЕНИЕ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ В ПРЕДУПРЕЖДЕНИИ КИБЕРПРЕСТУПНОСТИ

Албеков Шокир Адилбекович

Старший преподаватель цикла физической подготовки Институт повышения квалификации МВД Республики Узбекистан

shokiralbekov@gmail.com

Аннотация: В данной статье анализируется значение информационной культуры в предотвращении киберпреступности. Раскрыто понятие информационной культуры, ее роль и эффективность в предотвращении киберугроз. Также отмечается важность образования, продвижения и технологических решений для развития информационной культуры. Статья направлена на изучение инновационных подходов к обеспечению информационной безопасности и способов формирования информационной культуры в обществе.

Ключевые слова: киберпреступность, информационная культура, информационная безопасность, профилактика, цифровая грамотность, образование, пропаганда, технологические решения, киберриски, общественная безопасность.

THE IMPORTANCE OF INFORMATION CULTURE IN PREVENTING CYBERCRIME

Albekov Shokir Adilbekovich

Senior teacher of physical training cycle Institute for Advanced Studies of the Ministry of Internal Affairs of the Republic of Uzbekistan

shokiralbekov@gmail.com

Abstract: This article analyses the importance of information culture in preventing cybercrime. The concept of information culture, its role and effectiveness in preventing cyber threats are revealed. The importance of education, promotion and technological solutions for the development of information culture is also highlighted. The article is aimed at studying innovative approaches to information security and ways of forming information culture in society.

Keywords: cybercrime, information culture, information security, prevention, digital literacy, education, promotion, technological solutions, cyber risks, public safety.

КИРИШ. Рақамли технологиялар инсон ҳаётининг барча соҳаларига чуқур кириб борган ҳолда, ахборот хавфсизлигини таъминлаш долзарб масалага айланди. Кибержиноятчиликнинг ўсиши нафақат иқтисодий зарар, балки шахсий маълумотларнинг суиистеъмол қилиниши, ахборот ҳужумлари ва жамиятга бўлган ишончнинг пасайишига олиб келади. Ушбу мақолада

кибержиноятчиликка қарши профилактикада ахборот маданиятининг ўрни, уни шакллантириш усуллари ва амалий аҳамияти таҳлил қилинади.

Кибержиноятчиликнинг жамиятга таъсири.

1. Кибержиноятчилик турлари:

✓ Шахсий маълумотларни ўғирлаш (фишинг);

✓ Молиявий фирибгарлик;

✓ Дастурий таъминотга ҳужумлар ва зарарли кодлар тарқатиш;

✓ Сотиладиган маълумотлар базаларининг ноқонуний савдоси;

2. Жамиятга салбий таъсирлари:

✓ Давлат ва тижорат ташкилотлари фаолиятига зарар етказиш.

✓ Ахборотга ишончнинг пасайиши.

✓ Рақамли саводхонлик етишмаслиги туфайли кибержиноятлар қурбонларининг ортиши.

Ахборот маданияти нима ва нега у зарур?

1. Ахборот маданияти тушунчаси: Ахборот маданияти – инсоннинг ахборотни тўғри бошқариш, уни хавфсиз тарзда ишлатиш ва тарқатиш қобилиятидир. Ахборот хавфсизлиги қоидаларига риоя қилиш ва хавфларни олдиндан аниқлашга қаратилган билимлар тизими.

2. Ахборот маданиятининг аҳамияти:

➢ Фойдаланувчиларни киберхавфларга нисбатан ҳушёрликка чақириш.

➢ Киберхавфларни аниқлаш ва уларга қарши тезкор ҳаракат қилиш қобилиятини ошириш.

➢ Жамиятда ахборот ресурсларига бўлган масъулиятни ошириш.

Профилактик чора-тадбирлар ва ахборот маданиятини ривожлантиришда таълим ва тарғибот ишлари муҳим ўрин тутади, жумладан мактаб ва университетларда ахборот хавфсизлиги дарсларини жорий қилиш, ахборот маданияти бўйича оммавий маърифий тадбирлар ўтказиш орқали ижобий ютуқларга эришиш мумкин.

Шунингдек, ахборотни хавфсиз сақлаш ва шахсий маълумотларни муҳофаза қилиш бўйича ўқув қўлланмаларини тарқатиш, интернетдан хавфсиз фойдаланиш қоидалари бўйича вебинарлар ва тренинглар ташкил қилиш орқали ҳам рақамли саводхонликни ошириш мумкин.

Шу билан бирга хавфсизлик тизимлари ва антивирус дастурларини фойдаланишни тарғиб қилиш, киберҳужумларга қарши ҳимоя воситаларини жорий қилиш каби масалалар ахборот хавфсизлиги учун технологик чоралар сифатида қўлланилиши мақсадга мувофиқдир. Бундан ташқари киберхавфсизлик маданиятини шакллантириш ҳам муҳим омиллардан бири сифатида намоён бўлади, интернетда ўзаро ҳурмат ва одоб қоидаларига риоя қилиш, ёшлар ўртасида ахборот хавфсизлигига масъулиятли ёндашувни тарғиб қилиш ишлари шулар жумласига киритишимиз лозим.

ХУЛОСА. Ахборот маданияти кибержиноятчиликка қарши профилактик тадбирларнинг асосий йўналишларидан бири ҳисобланади. У жамият аъзоларининг ахборот хавфсизлигига бўлган ҳушёрлигини ошириб, шахсий ва жамоат ресурсларини ҳимоя қилишда самарали механизм ҳисобланади. Ахборот

маданиятини ривожлантириш орқали кибержиноятчиликни камайтириш, жамиятда хавфсиз рақамли муҳит яратиш имконияти юзага келади.

ТАВСИЯЛАР.

1. Мактаб ва олий таълим муассасаларида ахборот маданиятини шакллантирувчи махсус курслар ташкил этиш.

2. Ахборот хавфсизлиги қоидалари ҳақида оммавий ахборот воситалари орқали мунтазам тарғибот ишларини ўтказиш.

3. Давлат ва хусусий сектор ўртасида ахборот хавфсизлиги бўйича ҳамкорликни кучайтириш.

4. Интернет фойдаланувчиларининг ахборот хавфсизлигига доир хабардорлигини ошириш учун ижтимоий акциялар ўтказиш.

АДАБИЁТЛАР

1. Туркулец В.А. Информационная культура современного родителя как фактор предупреждения киберпреступлений в отношении несовершеннолетних. Материалы Третьего Международного научно-просветительского форума. Под общей редакцией С.Е.Туркулец, Е.В.Листопадовой. Хабаровск, 2022.
2. Карпова Д.Н. Киберпреступность: глобальная проблема и её решение. //журнал Власть, 2014.
3. Антонян Е.А. Противодействие киберпреступности. //Сборник статей по материалам IV Всероссийской научно-практической конференции. 2019.
4. Ҳасанова М.С. Рақамли саводхонлик: жамиятда ахборот маданиятини шакллантириш. // Жаҳон иқтисодиёти ва таълим, 2021.

KIBERJINOYATLARGA QARSHI KURASHDA XALQARO HAMKORLIKNING HUQUQIY ASOSLARI

Burxonov Bahodir Hayotovich

O‘zbekiston Respublikasi Ichki ishlar vazirligi
Malaka oshirish instituti Jismoniy tayyorgarlik sikli o‘qituvchisi

bahodirburxonov87@gmail.com

Annotatsiya: Ushbu maqolada XXI asrda kiberjinoyatlarning global miqyosda tarqalishi va ularni bartaraf etish uchun xalqaro hamkorlikning huquqiy asoslari tahlil qilinadi. Kiberjinoyatlar axborot texnologiyalaridan foydalanib amalga oshiriladigan huquqbuzarliklardir va ular davlatlararo xavfsizlik, iqtisodiy barqarorlik va fuqarolarni himoya qilish masalalariga jiddiy tahdid solmoqda. Maqolada BMT, INTERPOL, Evropa Ittifoqi kabi xalqaro tashkilotlar va “Kiberjinoyatlar to‘g‘risidagi Konventsiya” kabi xalqaro huquqiy hujjatlar orqali kiberjinoyatlarga qarshi kurashishda hamkorlikning muhim roli ko‘rsatilgan. Shuningdek, maqolada xalqaro hamkorlikning samaradorligini oshirishda duch kelinadigan huquqiy, siyosiy va texnologik muammolar ham tahlil qilinadi.

Kalit so‘zlar: Kiberjinoyat, xalqaro hamkorlik, huquqiy asoslar, BMT, INTERPOL, Evropa Ittifoqi, kiberxavfsizlik, kiberhujumlar, Budapeşt Konventsiya, xalqaro huquq.

ПРАВОВЫЕ ОСНОВЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ.

Бурхонов Баҳодир Ҳаётович

Преподаватель цикла физической подготовки Институт повышения квалификации Министерство внутренних дел Республики Узбекистан
bahodirburxonov87@gmail.com

Аннотация: В статье рассматриваются правовые основы международного сотрудничества в борьбе с киберпреступностью в условиях глобализации информационных технологий. Киберпреступления, совершаемые с использованием информационных технологий, представляют собой серьезную угрозу для безопасности государств, экономической стабильности и защиты граждан. Рассматривается роль таких международных организаций, как ООН, Интерпол, Европейский Союз, а также международных правовых документов, например, Конвенции о киберпреступности (Будапештская конвенция) в борьбе с киберпреступностью. В статье также анализируются проблемы, с которыми сталкиваются государства в процессе усиления международного сотрудничества в данной области.

Ключевые слова: Киберпреступность, международное сотрудничество, правовые основы, ООН, Интерпол, Европейский Союз, кибербезопасность, кибератаки, Будапештская конвенция, международное право.

LEGAL FOUNDATIONS OF INTERNATIONAL COOPERATION IN THE FIGHT AGAINST CYBERCRIME

Burkhonov Bahodir Hayotovich

Teacher of physical training cycle Institute of advanced training Ministry of Internal Affairs of the Republic of Uzbekistan
bahodirburxonov87@gmail.com

Abstract: This article examines the legal foundations of international cooperation in the fight against cybercrime in the context of the globalization of information technologies. Cybercrimes, committed using information technologies, pose serious threats to state security, economic stability, and the protection of citizens. The article explores the role of international organizations such as the UN, INTERPOL, the European Union, and international legal documents, such as the Cybercrime Convention (Budapest Convention), in combating cybercrime. The article also analyzes the challenges faced by countries in strengthening international cooperation in this area.

Keywords: Cybercrime, international cooperation, legal foundations, UN, INTERPOL, European Union, cybersecurity, cyberattacks, Budapest Convention, international law.

Kirish. XXI asrda global kommunikatsiya va axborot texnologiyalarining rivojlanishi kiberjinoyatlarning tez o‘sishiga olib keldi. Kiberjinoyatlar, internet tarmog‘i va raqamli texnologiyalar orqali amalga oshiriladigan harakatlar bo‘lib, ular davlatlararo xavfsizlik, iqtisodiy barqarorlik va fuqarolarni himoya qilish masalalariga jiddiy tahdid solmoqda. Kiberjinoyatlar global miqyosda keng tarqalganligi sababli, ular faqatgina milliy qonunchilik tizimlari doirasida emas, balki xalqaro hamkorlik va huquqiy asoslar orqali hal etilishi zarur. Ushbu maqolada kiberjinoyatlarga qarshi kurashda xalqaro hamkorlikning huquqiy asoslari tahlil qilinadi.

Kiberjinoyatlar va ularning xususiyatlari:

Kiberjinoyatlar – bu axborot texnologiyalaridan foydalanib, huquqbuzarliklar sodir etilishidir. Ular o‘z ichiga quyidagilarni oladi:

- Kompyuter tizimlariga noqonuniy kirish (hacking);
- Ma’lumotlarni o‘g‘irlash yoki yo‘qotish (data theft, data destruction);
- Onlayn firibgarlik, phishing;
- Kiberhujumlar va DDoS (Distributed Denial of Service) hujumlari;
- Raqamli identifikatsiya va moliyaviy xatoliklar.

Kiberjinoyatlarning ko‘plab turlari mavjud bo‘lib, ular fuqarolar, kompaniyalar va davlatlarga katta iqtisodiy va xavfsizlik xavfini tug‘diradi.

Kiberjinoyatlarga qarshi kurashda xalqaro hamkorlik.

Kiberjinoyatlarga qarshi samarali kurashish faqat milliy qonunlar bilan cheklanishi mumkin emas. Bu masala global miqyosda hal qilinishi kerak. Xalqaro hamkorlik bu jarayonda muhim ahamiyatga ega. Xalqaro huquqiy asoslar, bir tomonlama va ko‘p tomonlama bitimlar, shuningdek, mamlakatlar o‘rtasidagi tashkilotlar va formlar kiberjinoyatlarga qarshi kurashishda qo‘llaniladigan asosiy vositalardir.

BMT va xalqaro xavfsizlik tashkilotlari. Birlashgan Millatlar Tashkiloti (BMT) va uning tarkibidagi idoralar, jumladan, BMTning axborot xavfsizligi bo‘yicha maxsus komissiyasi, kiberjinoyatlarga qarshi kurashda asosiy ro‘l o‘ynaydi. BMT tomonidan qabul qilingan hujjatlar, masalan, “Kiberxavfsizlik to‘g‘risidagi rezolyutsiyalar” ko‘plab davlatlarni kiberjinoyatlarga qarshi kurashga undaydi va xalqaro hamkorlikni rivojlantirishga yordam beradi.

Xalqaro politsiya tashkiloti – INTERPOL. INTERPOL kiberjinoyatlarga qarshi kurashishda muhim rol o‘ynaydi. INTERPOLning kiberjinoyatlarga qarshi bo‘limi, davlatlar o‘rtasida axborot almashinuvi va kiberhujumlarni aniqlash bo‘yicha o‘zaro hamkorlikni kuchaytirishga yordam beradi. INTERPOLning xalqaro ishlari asosan kiberjinoyatlar bo‘yicha tezkor ma’lumotlarni uzatish, tajriba almashish va o‘rganish, shuningdek, huquqni muhofaza qiluvchi idoralar o‘rtasida tizimli aloqalarni o‘rnatishdan iborat.

Evropa Ittifoqi va kiberxavfsizlikni ta’minlash. Evropa Ittifoqi (EI) kiberjinoyatlar bilan kurashda faollik ko‘rsatib keladi. 2013-yilda Evropa Ittifoqi kiberjinoyatlarga qarshi kurashish uchun Evropa Komissiyasi tomonidan ishlab chiqilgan “Kiberxavfsizlik strategiyasi”ni qabul qildi. Shuningdek, Evropa Kiberjinoyatlar Markazi (EC3) va Evropa Xavfsizlik va Hamkorlik Agentligi (ENISA) orqali kiberjinoyatlarga qarshi kurashishni kuchaytirish uchun bir qator faoliyatlar amalga oshiriladi.

Kiberjinoyatlarni jinoiy javobgarlikka tortish. Kiberjinoyatlarga qarshi kurashda xalqaro jinoiy huquq muhim ahamiyatga ega. 2001-yilda Istanbulda “Kiberjinoyatlar to‘g‘risidagi Konvensiya” (Budapeşt Konvensiya) imzolandi. Bu xalqaro huquqiy hujjat, kiberjinoyatlar bilan bog‘liq bo‘lgan huquqbuzarliklarni jinoyat deb hisoblashni va ular uchun javobgarlikni belgilaydi. Ushbu Konvensiya davlatlar o‘rtasida kiberjinoyatlarni tergov qilish, jinoyatchilarni jazolash, hamda axborot xavfsizligini ta’minlashda hamkorlikni kuchaytirishga yo‘naltirilgan.

Xalqaro hamkorlikda kuzatiladigan muammolar:

Huquqiy muvofiqlikning yo‘qligi. Turli mamlakatlarda kiberjinoyatlar bo‘yicha huquqiy tartiblar bir-biridan farq qiladi. Ba’zi davlatlar kiberjinoyatlar bilan kurashishda faol bo‘lsa, boshqalari bunday jinoyatlar haqida yetarlicha qonunlar qabul qilmagan yoki amaldagi qonunlarni samarali amalga oshirishda qiyinchiliklarga duch kelmoqda.

Ijtimoiy va siyosiy omillar. Kiberjinoyatlarga qarshi kurashda ba’zi davlatlar o‘zlarining siyosiy yoki iqtisodiy manfaatlarini ilgari surib, xalqaro hamkorlikni sustlashtirishlari mumkin. Bu holat, ayniqsa, davlatlar o‘rtasida ma’lumot almashish va jinoyatchilarni ekstraditsiya qilish masalalarida muammolarni keltirib chiqarishi mumkin.

Texnologik taraqqiyot va yangi tahdidlar. Texnologiyalar tez rivojlanayotgan bir paytda, kiberjinoyatlar ham doimiy ravishda yangi shakllarini kasb etmoqda. Bu holat, kiberjinoyatlarga qarshi kurashishda xalqaro hamkorlikni samarali amalga oshirishni yanada qiyinlashtiradi.

Xulosa

Kiberjinoyatlarga qarshi kurashda xalqaro hamkorlikning huquqiy asoslari mavjud bo‘lib, bu jarayonda xalqaro huquqiy hujjatlar, shuningdek, davlatlar o‘rtasidagi tashkilotlar va tashkilotlararo aloqalar muhim rol o‘ynaydi. Kiberjinoyatlar, global tahdid bo‘lgani sababli, ularni bartaraf etish uchun mamlakatlar o‘rtasida yaqin hamkorlik, huquqiy asoslar va zamonaviy texnologiyalarni qo‘llash zarur. Shu bilan birga, kiberjinoyatlar bilan kurashishda mavjud muammolarni hal qilish uchun yanada kuchli hamkorlik va yaxshilangan huquqiy asoslar zarur bo‘ladi.

ADABIYOTLAR:

1. BMT Xavfsizlik Kengashining kiberxavfsizlik bo‘yicha rezolyutsiyalari. Birlashgan Millatlar Tashkiloti, 2020. – https://www.un.org/securitycouncil/
2. “Kiberxavfsizlik: BMT va davlatlarning hamkorligi”. BMT, 2021. – https://www.un.org/cybersecurity
3. “Budapesht Konventsiya: Kiberjinoyatlarga Qarshi Kurashishda Xalqaro Hamkorlik”. Evropa Kengashi, 2001. https://www.coe.int/en/web/cybercrime /the-budapest-convention
4. Kiberjinoyatlar va ularni tergov qilish. INTERPOL, 2022. – https://www.interpol.int/en/Crimes/Cybercrime
5. “Evropa Ittifoqining Kiberxavfsizlik Strategiyasi”. Evropa Komissiyasi, 2013. – https://ec.europa.eu/digital-strategy/our-policies/cybersecurity_en
6. M.O‘tkir, A.Rustamov. “Kiberjinoyatlarga Qarshi Kurashda Xalqaro Huquqiy Asoslar”. Tashkent, 2019.

7. A.Smith. International Cybersecurity Law. Oxford University Press, 2018.
8. J.S.Lewis. “Kiberjinoyatlar va huquqiy javobgarlik: Global va milliy nuqtai nazar”. Harvard University Press, 2020.
9. M.Green. “Xalqaro Huquq va Kiberjinoyatlar”. Cambridge University Press, 2019.
10. A.Brooks. “Cybersecurity and International Law: A Comprehensive Overview”. Springer, 2021.
11. “The Role of Interpol in Combating Cybercrime”. International Law Review, 2020.
12. “The EU's Strategy on Cybersecurity: Legal and Institutional Frameworks”. European Union Law Journal, 2022.
13. “Cybercrime and the Protection of International Borders”. Journal of International Security, 2021.
14. L.White. “Digital Security and Global Cooperation: Emerging Legal Challenges”. Oxford University Press, 2017.
15. “International Law and the Fight Against Cybercrime: A Comparative Perspective”. Journal of Comparative and International Law, 2022.

ВЛИЯНИЕ КИБЕРПРЕСТУПЛЕНИЙ НА ОБЩЕСТВО

Усманов Алишер Шарафиддинович

Начальник цикла физической подготовки Институт повышения квалификации МВД Республики Узбекистан

Аннотация: Киберпреступления стали одной из наиболее актуальных угроз современному обществу. Они затрагивают не только финансовую и экономическую сферы, но и личную безопасность, доверие к технологиям и психологическое состояние граждан. В данной статье исследуются основные типы киберпреступлений и их последствия для общества, рассматриваются правовые и социальные аспекты, а также предлагаются меры по минимизации их негативного влияния.

Ключевые слова: киберпреступления, информационная безопасность, цифровая экономика, киберугрозы, социальные последствия, психологическое воздействие, финансовые потери, кибербуллинг, утечка данных, правовые аспекты, цифровая грамотность, международное сотрудничество, профилактика киберпреступлений.

КИБЕРЖИНОЯТЛАРНИНГ ЖАМИЯТГА ТАЪСИРИ

Усманов Алишер Шарафиддинович

Ўзбекистон Республикаси Ички ишлар вазирлиги Малака ошириш институти Жисмоний тайёргарлик цикли бошлиғи

Аннотация: Кибержиноятлар замонавий жамият учун энг долзарб таҳдидлардан бирига айланди. Улар нафақат молиявий ва иқтисодий соҳаларга, балки шахсий хавфсизлик, технологияга ишонч ва фуқароларнинг психологик ҳолатига ҳам таъсир қилади. Ушбу мақолада кибержиноятларнинг асосий турлари ва уларнинг жамият учун оқибатлари кўриб чиқилади, ҳуқуқий ва ижтимоий жиҳатлар кўриб чиқилади, шунингдек, уларнинг салбий таъсирини минималлаштириш чоралари таклиф этилади.

Калит сўзлар: кибержиноятлар, ахборот хавфсизлиги, рақамли иқтисодиёт, кибертаҳдидлар, ижтимоий оқибатлар, психологик таъсирлар, молиявий йўқотишлар, кибербуллинг, маълумотларнинг сизиб чиқиши, ҳуқуқий жиҳатлар, рақамли саводхонлик, халқаро ҳамкорлик, кибержиноятларнинг олдини олиш.

IMPACT OF CYBERCRIME ON SOCIETY

Usmanov Alisher Sharafiddinovich

Head of physical training cycle Institute for Advanced Training of the Ministry of Internal Affairs of the Republic of Uzbekistan

Abstract: Cybercrimes have become one of the most pressing threats to modern society. They affect not only financial and economic spheres, but also personal security, trust in technology and psychological state of citizens. This article explores the main types of cybercrimes and their consequences for society, considers legal and social aspects, and proposes measures to minimise their negative impact.

Keywords: cybercrime, information security, digital economy, cyberthreats, social consequences, psychological impact, financial losses, cyberbullying, data leakage, legal aspects, digital literacy, international cooperation, cybercrime prevention.

ВВЕДЕНИЕ. В эпоху цифровой трансформации технологии становятся неотъемлемой частью жизни каждого человека. Однако наряду с их преимуществами наблюдается рост киберпреступлений, представляющих серьезную угрозу обществу. Актуальность исследования заключается в том, что последствия киберпреступлений охватывают не только экономическую, но и социальную сферу, нанося ущерб личной безопасности и общественным ценностям.

Цель статьи - анализ влияния киберпреступлений на общество и поиск эффективных путей их предотвращения.

Основные типы киберпреступлений. Киберпреступления могут принимать множество форм, наиболее распространенными из которых являются:

1. Кража данных. Хакеры похищают личную и финансовую информацию, что приводит к утечке данных и финансовым потерям.

2. Финансовые мошенничества. Фишинговые атаки и скимминг наносят ущерб как частным лицам, так и организациям.

3. Кибербуллинг. Социальные сети становятся площадкой для травли, что влияет на психическое здоровье пользователей.

4. Атаки на инфраструктуру. Критически важные объекты, такие как энергетические и транспортные системы, становятся мишенью для кибератак.

Киберпреступления ежегодно наносят мировой экономике ущерб в триллионы долларов. Компании вынуждены увеличивать расходы на кибербезопасность, а частные лица сталкиваются с финансовыми потерями. Снижение доверия к цифровым платформам ведет к замедлению темпов цифровизации.

Кроме того, киберпреступления оказывают значительное влияние на социальную сферу:

- Психологическое давление. Жертвы кибербуллинга и мошенничеств испытывают стресс, тревогу и потерю уверенности.

- Угроза личной безопасности. Утечка данных приводит к риску шантажа или идентификационного мошенничества.

- Социальная изоляция. Потеря доверия к онлайн-среде может снизить уровень социальной активности.

Противодействие киберпреступлениям осложняется их транснациональным характером. Отсутствие единой законодательной базы и недостаточное международное сотрудничество затрудняют расследование и преследование киберпреступников.

Диаграмма № 1. Распределение типов преступлений.

Пути минимизации ущерба. Для эффективной борьбы с киберпреступлениями необходим комплексный подход:

1. Повышение цифровой грамотности. Обучение населения основам безопасного поведения в интернете.
2. Усиление законодательной базы. Разработка международных стандартов и ужесточение наказаний за киберпреступления.
3. Использование современных технологий. Внедрение систем искусственного интеллекта для выявления и предотвращения угроз.

ЗАКЛЮЧЕНИЕ. Киберпреступления представляют собой серьезную угрозу для современного общества, оказывая негативное воздействие на экономику, личную безопасность и социальные связи. Борьба с этим явлением требует скоординированных усилий со стороны государств, бизнеса и общества. Увеличение осведомленности о киберугрозах и использование передовых технологий могут минимизировать их последствия и создать безопасную цифровую среду.

ЛИТЕРАТУРА

1. Кобец П.Н. Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения. // Вестник Самарского юридического института, 2022.
2. Богданов А.В. Основные направления деятельности полиции по предупреждению и профилактике правонарушений среди несовершеннолетних. // Вестник Московского университета МВД России, 2017.
3. Базаров Р.Т., Файзуллина Л.А., Клементьев М.М. Влияние киберпреступлений на экономическую безопасность страны на примере Российской Федерации // Экономика и менеджмент, 2022.
4. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны: Пер. с анг., 2020.
5. Масалков А.С. Особенности киберпреступлений: инструменты нападения и защиты информации. 2018.
6. Чернова Е.В. Информационная безопасность человека: Учебное пос. для вузов. 2022.

СОЦИАЛЬНЫЕ АСПЕКТЫ КИБЕРПРЕСТУПНОСТИ

Албеков Шокир Адилбекович

Старший преподаватель цикла физической подготовки Институт повышения квалификации МВД Республики Узбекистан

shokiralbekov@gmail.com

Аннотация: Статья посвящена анализу социальных аспектов киберпреступности, включая психологический портрет киберпреступников, использование методов социальной инженерии и их последствия для общества. Рассматриваются основные мотивации и стратегии преступников, такие как фишинг, вишинг и претекстинг, а также влияние кибератак на социальные

институты и отдельных граждан. Особое внимание уделяется проблемам недоверия к технологиям, социальной изоляции жертв и распространению дезинформации. В статье предложены меры для минимизации негативных последствий киберпреступности, включая повышение цифровой грамотности, развитие технологий защиты, поддержку жертв и укрепление законодательства.

Ключевые слова: киберпреступность, социальные аспекты, социальная инженерия, психология киберпреступников, влияние кибератак, цифровая грамотность, кибербезопасность, дезинформация.

КИБЕРЖИНОЯТНИНГ ИЖТИМОИЙ ЖИҲАТЛАРИ

Албеков Шокир Адилбекович

Ўзбекистон Республикаси Ички ишлар вазирлиги Малака ошириш институти Жисмоний тайёргарлик цикли катта ўқитувчиси

shokiralbekov@gmail.com

Аннотация: Мақола кибержиноятчиликнинг ижтимоий жиҳатларини, жумладан кибержиноятчиларнинг психологик портретини, ижтимоий муҳандислик усулларидан фойдаланишни ва уларнинг жамият учун оқибатларини таҳлил қилишга бағишланган. Жиноятчиларнинг асосий мотивлари ва стратегиялари, масалан, фишинг, вишинг ва претекстинг, шунингдек, киберҳужумларнинг ижтимоий институтлар ва алоҳида фуқароларга таъсири кўриб чиқилади. Технологияга ишончсизлик, жабрланганларни ижтимоий четлаштириш ва дезинформацияни тарқатиш муаммоларига алоҳида эътибор қаратилмоқда. Мақолада кибержиноятларнинг салбий оқибатларини минималлаштириш, жумладан, рақамли саводхонликни ошириш, ҳимоя технологияларини ишлаб чиқиш, жабрланувчиларни қўллаб-қувватлаш ва қонунчиликни мустаҳкамлаш чора-тадбирлари таклиф этилган.

Калит сўзлар: кибержиноят, ижтимоий жиҳатлар, ижтимоий муҳандислик, кибержиноятчилар психологияси, киберҳужумларнинг таъсири, рақамли саводхонлик, киберхавфсизлик, дезинформация.

SOCIAL ASPECTS CYBERCRIME

Albekov Shokir Adilbekovich

Senior teacher of physical training cycle Institute for Advanced Studies of the Ministry of Internal Affairs of the Republic of Uzbekistan

shokiralbekov@gmail.com

Abstract: This article analyses the social aspects of cybercrime, including the psychological profile of cybercriminals, the use of social engineering techniques and their consequences for society. The main motivations and strategies of criminals, such as phishing, vishing and pre-texting, as well as the impact of cyberattacks on social institutions and individual citizens are examined. Particular attention is paid to the

problems of distrust in technology, social isolation of victims, and the spread of misinformation. The article suggests measures to minimise the negative effects of cybercrime, including increasing digital literacy, developing protection technologies, supporting victims and strengthening legislation.

Keywords: cybercrime, social aspects, social engineering, psychology of cybercriminals, impact of cyberattacks, digital literacy, cybersecurity, disinformation.

ВВЕДЕНИЕ. Киберпреступность в XXI веке стала неотъемлемой частью информационного общества, затрагивая все аспекты жизни человека. Она не только угрожает экономике и государственной безопасности, но и оказывает значительное влияние на социальную сферу. Одним из ключевых аспектов является использование социальной инженерии и влияние кибератак на общество, а также психологический портрет киберпреступников. Настоящая статья посвящена анализу этих аспектов с целью выявления их социальных последствий и возможных методов противодействия.

Психология киберпреступников.

Киберпреступники представляют собой разнородную группу, в которую входят как отдельные личности, так и организованные группы. Исследования показывают, что мотивация преступников может быть разнообразной:

1. Финансовая выгода. Большинство кибератак направлено на кражу средств или шантажа.

2. Желание признания. Молодые хакеры нередко совершают атаки ради демонстрации своих технических возможностей.

3. Идеологические мотивы. Кибератаки могут быть связаны с политическими или религиозными взглядами, часто служа инструментом кибертерроризма.

4. Протест или месть. Некоторые атакуют организации, с которыми имеют личные или профессиональные конфликты.

Психологический портрет часто включает следующие черты: высокий уровень интеллекта, отсутствие эмпатии, умение абстрагироваться от последствий своих действий, а также склонность к риску.

Диаграмма №1. Разнообразие мотивации преступников.

Социальная инженерия: методы и последствия.

Социальная инженерия - это манипулятивные техники, которые используют человеческую психологию для получения доступа к конфиденциальной информации. Рассмотрим методы социальной инженерии:

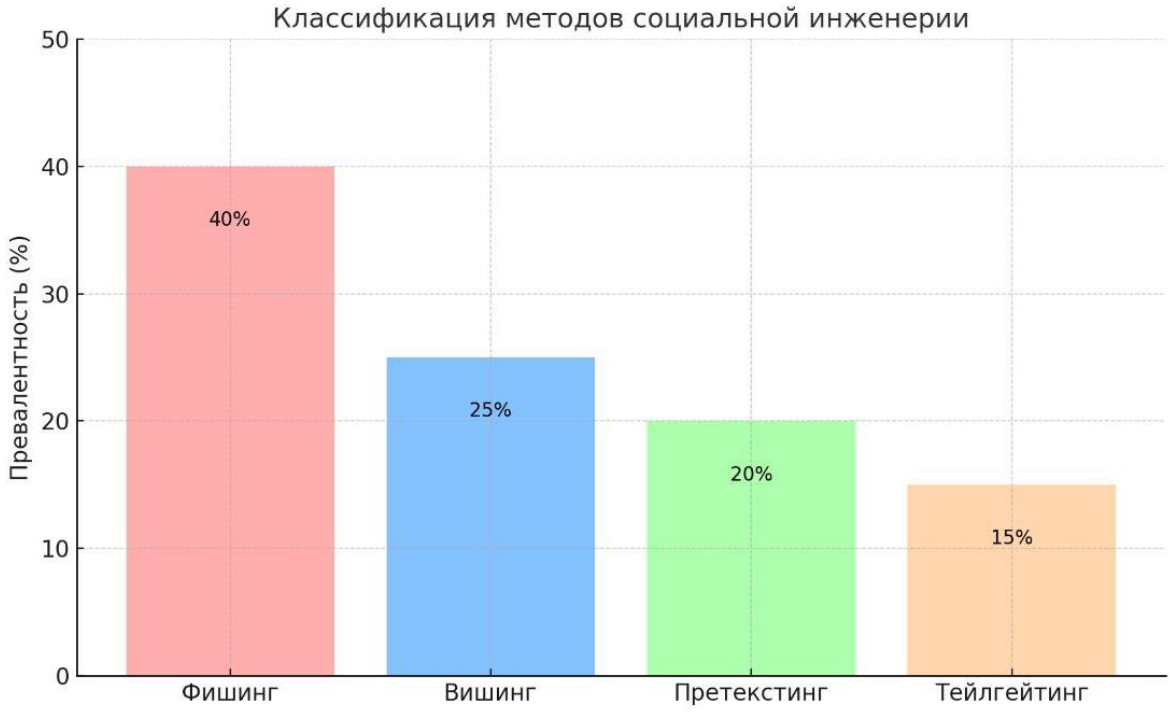
✓ Фишинг: рассылка электронных писем или сообщений с целью обмана пользователя;

✓ Вишинг: телефонные звонки с целью выманивания данных;

✓ Претекстинг: создание ложной ситуации для получения доверия;

✓ Тейлгейтинг: использование физического проникновения, например, следование за сотрудником в офис.

Диаграмма №2. Классификация методов социальной инженерии.



Социальные последствия:

➢ Потеря доверия к цифровым технологиям;

➢ Ущерб психическому здоровью жертв;

➢ Усиление цифрового неравенства: люди с низкой цифровой грамотностью более подвержены атакам.

Влияние кибератак на общество.

Кибератаки стали причиной значительных социальных изменений, включая:

❖ Рост недоверия к технологиям.

❖ Масштабные утечки данных (например, атак на Facebook или банковские системы) подрывают доверие пользователей к цифровым сервисам.

❖ Социальная изоляция. Жертвы мошенничества в сети могут испытывать чувство стыда, что приводит к социальной замкнутости.

❖ Распространение дезинформации. Кибератаки все чаще используются для манипуляции общественным мнением, особенно в период выборов.

Пути минимизации социальных последствий киберпреступности.

1. Повышение цифровой грамотности. Необходимо внедрять образовательные программы, направленные на обучение безопасному поведению в интернете.

2. Развитие технологий защиты. Использование современных систем идентификации, например, многофакторной аутентификации.

3. Поддержка жертв. Организация психологической помощи и консультаций для пострадавших от кибератак.

4. Укрепление законодательства. Международное сотрудничество в области кибербезопасности может способствовать эффективному противодействию преступникам.

ЗАКЛЮЧЕНИЕ. Киберпреступность оказывает значительное влияние на социальные аспекты жизни, затрагивая не только жертв, но и общество в целом. Понимание мотивации преступников, методов социальной инженерии и последствий кибератак является ключом к эффективной борьбе с этим явлением. Только комплексный подход, включающий образовательные, технологические и законодательные меры, способен минимизировать социальные последствия киберпреступности.

СПИСОК ЛИТЕРАТУРЫ

1. Муминов М. Понятие киберпреступности и ее социальная опасность. // Общество и инновации. 2024.
2. O‘zbekiston Respublikasining 2022-yil 15-aprel kunidagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son qonuni.
3. Niyozova S.S. Kiberjinoyatchilik. // O‘quv qo‘llanma T.:TDYU nashriyoti, 2024.
4. Касперский Е.В. Атака на доверие: Как социальная инженерия стала главной угрозой цифровой эры // Кибербезопасность: Технологии и практика. 2022.
5. Коменский Н.А. Компьютерная информация и информационные технологии как средство совершения преступления. // Преступления в информационной сфере: проблемы расследования, квалификации, реализации ответственности и предупреждения: материалы международной научно-практической конференции 14-15 февраля 2013 г.

KIBERJINOYATCHILIK VA UNGA QARSHI KURASHISHNING TAHLILI

Muslimov Xusan Nishonboyevich

Malaka oshirish instituti Jangovar tayyorgarlik sikli o‘qituvchisi

Annotatsiya. Ushbu tezisda muallif O‘zbekiston Respublikasdida kiberjinoyatchilik va unga qarshi kurashish bo‘yicha normativ-huquqiy hujjatlarning tahlilini amalga oshiradi. Tezisda O‘zbekiston Respublikasining “Normativ-huquqiy hujjatlar to‘g‘risida”gi Qouninng normalarida ifodalangan normativ-huquqiy

hujjatlarning aynan kiberxavfsizlikka oid bo‘lgan qismini amaliy misollar bilan tahlil qilingan.

Kalit so‘zlar: kiberjinoyatchilik, kibermuhit, jinoyat, jinoyatchilikka qarshi kurashish, normativ-huquqiy hujjatlar.

Texnika-texnologiyalar rivoj topgani bilan ulardan foydalanish maqsadlari ham tubdan o‘zgarib bormoqda. Demandsage.com saytining statistik ma’lumotlariga qaraganda hozirda O‘zbekistonda 18 milliondan ortiq “Telegram”messenjeri foydalanuvchilari ro‘yxatdan o‘tgan hisoblanadi. Shuningdek, Telegram haqidagi mualliflik kanali asoschisi, rossiyalik Georgiy Lobushkin ijtimoiy tarmoqning O‘zbekistondagi statistikasini ma'lum qildi. Uning ta’kidlashicha, O‘zbekiston Telegram kanallari soni bo‘yicha Rossiyadan keyin ikkinchi o‘ringa chiqib olgan.

Shunday qilib, O‘zbekiston Telegram kanallari soni va ularning auditoriyasi bo‘yicha Rossiyadan keyin ikkinchi o‘rinda turadi. O‘zbekistonda Telegram kanallarining umumiy auditoriyasi 740 990 000 kishini tashkil qiladi. Undan tashqari, O‘zbekistonda Telegram bozori juda faol rivojlanmoqda va juda istiqbolli ko‘rinadi. Shuning uchun ham hozir O‘zbekistonda 123 mingdan ortiq Telegram kanali, 18 mingga yaqin chat bor. Shu bilan birga, datareportal.com saytining ma’lumotlariga ko‘ra 2023-yil yanvar oyida O‘zbekistonda 5,35 million ijtimoiy tarmoq foydalanuvchisi ro‘yxatdan o‘tgan bo‘lib, bu umumiy aholining 15,3 foizini tashkil etadi. Ko‘rinib turibdiki, hozirgi kunda internet jahon tarmog‘idan foydalanuvchilar soni hamda ko‘lami tobora ortib bormoqda. Biroq bunga mos va proporsional tarzda bu tarmoqlardan o‘zlarining g‘arazli maqsadlari yo‘lida ham foydalanib ko‘pchilik aholining yostig‘ini quritayotgan ishbilarmonlar ham talaygina.

Jumladan, so‘zga olingan telegram ijtimoiy messenjeri orqali so‘nggi 3 yil ichida sodir etilgan jinoyatlarning soni va u orqali yetkazilgan zararning miqdori keskin oshganligini ko‘rish mumkin. Jumladan, 2023-yilning 23-iyul sanasida IIV.uz saytida berilgan ma’lumotga ko‘ra: “Samarqand viloyati Pastdarg‘om tumanida yashovchi 48 yoshli Yu.B. murojaat qilib, o‘ziga tegishli bo‘lgan mobil telefon qurilmasini yo‘qotib qo‘yganligi va bank kartasidan 2.220.000 so‘m pullari noma’lum shaxs tomonidan yechib olinganligini ma’lum qilgan. Tezkor qidiruv xizmati Kiberxavfsizlik bo‘linmalari xodimlari tomonidan o‘tkazilgan tezkor-qidiruv tadbirlari natijasida, mazkur jinoyatni Toshkent shahar Yunusobod tumanida yashovchi 32 yoshli R.K. sodir etganligi aniqlangan. Gumonlanuvchi sifatida tergov organlariga jalb etilgan, R.K. jabrlanuvchi mobil telefon qurilmasini topib olgach undagi “SIM-karta”ni o‘z telefoniga faollashtirgan holda bank kartasi boshqaruvini qo‘lga kiritib ushbu jinoyatni amalga oshirganligi aniqlangan. Mazkur holat yuzasidan O‘zbekiston Respublikasi JKning 169-moddasi 3-qismi bilan jinoyat ishi qo‘zg‘atilib, dastlabki tergov harakatlari olib borilmoqda”-deya bayon etilgan. Ko‘rinib turibdiki, oddiy ehtiyotsizlik yuzasidan yo‘qotilgan sim karta ortidan shaxs o‘z maqsadida jinoyatga qo‘l urmoqda. Bunda esa kibermuhitning keng imkoniyatlari jinoyat sodir etishga yordam bermoqda. Bu kabi jinoyatlarning kunda, kun ora sodir etilishi, avvalo bu jinoyatlar o‘zi qanday jinoyat hamda bu jinoyatlarga nisbatan qanday javobgarlik belgilanganligini tahlil qilish zaruratini yuzaga keltiradi.

O‘zbekiston Respublikasi Jinoyat kodeksining 2-moddasiga ko‘ra: “shaxsni, uning huquq va erkinliklarini, jamiyat va davlat manfaatlarini, mulkni, tabiiy muhitni,

tinchlikni, insoniyat xavfsizligini jinoiy tajovuzlardan qo‘riqlash, shuningdek jinoyatlarning oldini olish, fuqarolarni respublika Konstitutsiyasi va qonunlariga rioya qilish ruhida tarbiyalash”- Jinoyat kodeksining vazifalari ekanligi belgilab qo‘yilgan. Demak, shaxs yoki uning hayotiga, yoki mulkka, shuningdek konstitutsiyaviy tuzumga qilingan har qanday suiqasd hamda ijtimoiy xavfli qilmish jinoyat kodeksida belgilangan javobgarlikni qo‘llash orqali jinoyat deb qabul qilinar ekan. Biz mavzuyimiz doirasida kibermuhitda sodir etilgan jinoyatlar uchun qonunchiligimizda belgilangan javobgarlik masalarini tahlil qilayotganimiz asnosida, o‘zi kibermuhit va kiberjinoyat nima degan savollarga qonunchiligimizdan javob olsak. O‘zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashlarning huquqiy asoslarini yaratish hamda qonunchilik darajasida tartibga solish maqsadida 2022 yil 15 apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ 764-son maxsus qonunni qabul qilinganligini alohida ta’kidlash zarur. Ushbu Qonunning maqsadi kiberxavfsizlik sohasidagi munosabatlarni tartibga solishdan iborat. Qonunda bir qator tushunchalarga qonuniy tasnif va ta’riflar berilgan. Ular quyidagilar:

kiberjinoyatchilik — axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi;

kibermakon — axborot texnologiyalari yordamida yaratilgan virtual muhit; kibertahdid — kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui;

kiberxavfsizlik — kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati; kiberxavfsizlik hodisasi — kibermakonda axborot tizimlarining ishlashida uzilishlarga va (yoki) ulardagi axborotning ochiqligi, yaxlitligi va undan erkin foydalanilishining buzilishiga olib kelgan hodisa;

kiberxavfsizlik obyekti — axborotning kiberhimoya qilinishini hamda milliy axborot tizimlari va resurslarining kiberxavfsizligini ta’minlashga doir faoliyatda foydalaniladigan axborot tizimlari majmui, shu jumladan muhim axborot infratuzilmasi obyektlari;

kiberxavfsizlik subyekti — milliy axborot resurslariga ega bo‘lish, ulardan foydalanish va ularni tasarruf etish hamda ulardan foydalanish bo‘yicha elektron axborot xizmatlari ko‘rsatish, axborotni himoya qilish hamda kiberxavfsizlik bilan bog‘liq muayyan huquqlar va majburiyatlarga ega bo‘lgan yuridik shaxs va (yoki) yakka tartibdagi tadbirkor, shu jumladan muhim axborot infratuzilmasi subyektlari;

kiberhimoya — kiberxavfsizlik hodisalarining oldini olishga, kiberhujumlarni aniqlashga va ulardan himoya qilishga, kiberhujumlarning oqibatlarini bartaraf etishga, telekommunikatsiya tarmoqlari, axborot tizimlari hamda resurslari faoliyatining barqarorligini va ishonchliligini tiklashga qaratilgan huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik chora-tadbirlar, shuningdek ma’lumotlarni kriptografik va texnik jihatdan himoya qilish chora-tadbirlari majmui;

kiberhujum — kibermakonda apparat, apparat-dasturiy va dasturiy vositalardan foydalangan holda qasddan amalga oshiriladigan, kiberxavfsizlikka tahdid soladigan harakat; muhim axborot infratuzilmasi — muhim strategik va

ijtimoiy-iqtisodiy ahamiyatga ega bo‘lgan avtomatlashtirilgan boshqaruv tizimlarining, axborot tizimlari hamda tarmoqlar va texnologik jarayonlar resurslarining majmui;

muhim axborot infratuzilmasi obyektlari — davlat boshqaruvi va davlat xizmatlari ko‘rsatish, mudofaa, davlat xavfsizligini, huquq-tartibotni ta’minlash, yoqilg‘i-energetika majmui (atom energetikasi), kimyo, neft-kimyo tarmoqlari, metallurgiya, suvdan foydalanish va suv ta’minoti, qishloq xo‘jaligi, sog‘liqni saqlash, uy-joy kommunal xizmatlar ko‘rsatish, bank-moliya tizimi, transport, axborot-kommunikatsiya texnologiyalari, ekologiya va atrof-muhitni muhofaza qilish, strategik ahamiyatiga ega bo‘lgan foydali qazilmalarni qazib olish va qayta ishlash sohasida, ishlab chiqarish sohasida, shuningdek iqtisodiyotning boshqa tarmoqlarida va ijtimoiy sohada qo‘llaniladigan axborotlashtirish tizimlari;

muhim axborot infratuzilmasi subyektlari — davlat organlari va tashkilotlari, shuningdek mulk, ijara huquqlari asosida yoki boshqa qonuniy asoslarda muhim axborot infratuzilmasi obyektlariga egalik qiluvchi yuridik shaxslar, shu jumladan muhim axborot infratuzilmasi obyektlarining ishlashini hamda hamkorligini ta’minlovchi yuridik shaxslar va (yoki) yakka tartibdagi tadbirkorlar.

Ta’riflardan ko‘rinib turibdiki, kiberjinoyatchilik — axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi hisoblanadi. Shunday ekan. Qaysi jinoyatlar internet tarmog‘i, kiberhimoya dasturiy ta’minot vositalalari, texnika vositalaridan foydalangan holda sodir etilishi haqida tahlil yuritish maqsadga muvofqdir. “Kiberxavfsizlik to‘g‘risida”gi O‘zbekiston Respublikasining kibermakonda sodir etilgan jinoyatlarga nisbatan javobgarlik belgilangan qonun hujjatlari hisoblanar ekan. So‘nggi paytlarda ijtimoiy tarmoqlarda saytlarni buzib kirish, virusli dasturlar tarqatish kabi holatlar haqida xabarlar ko‘paydi. Kiberj inoyatlar, ayniqsa, pandemiya vaqtida jiddiy muammolardan biriga aylangan edi. Jinoyat kodeksining bir qator moddalarida kompyuter texnikasi vositalaridan foydalanib sodir etiladigan jinoyatlar va ularga nisbatan javobgarlik ko‘zda tutilgan. Jumladan, ushbu kodeksning 278[5]-moddasiga ko‘ra, o‘zganing kompyuter 83 uskunasini qasddan ishdan chiqarish, xuddi shuningdek kompyuter tizimini buzish (kompyuter sabotaji): 3 yilgacha muayyan huquqdan mahrum qilib, 66 mln 900 ming so‘mdan 89 mln 200 ming so‘mgacha miqdorda jarima; 2 yilgacha ozodlikni cheklash; 2 yilgacha ozodlikdan mahrum qilish bilan jazolanadi deb belgilab qo‘yilgan. Shuningdek, mazkur harakatlarni guruh bo‘lib, takroran yoki xavfli retsidivist tomonidan sodir etish 3 yilgacha ozodlikdan mahrum qilish bilan jazolashga sabab bo‘lishi mumkin6. Shuningdek, qaysi jinoyatlar kibermuhitda ham sodir etilishi mumkinligi va ularga nisbatan belgilangan jazo choralarini tahlil qilamiz. Ko‘rinib turibdiki, hozirgi kunda kiberjinoyatchilik asosan mulkiy jinoyatlarda fribgarlik, talonchilik, tovlamachilik, undan tashqari pornografik, irqiy ayirmachilik, buzg‘unchilik go‘yalarini targ‘ib qiluvchi materiallarni tayyorlash, saqlash hamda tarqatish kabi jinoyatlrda ko‘plab uchramoqda. O‘zbekiston Respublikasi Jinoyat kodeksning 165-moddasiga ko‘ra: Tovlamachilik, ya’ni jabrlanuvchi yoki uning yaqin kishilariga zo‘rlik ishlatish, mulkka shikast yetkazish yoki uni nobud qilish yoxud jabrlanuvchi uchun sir saqlanishi lozim bo‘lgan

ma’lumotlarni oshkor qilish bilan qo‘rqitib o‘zgadan mulkni yoki mulkiy huquqni topshirishni, mulkiy manfaatlar berishni yoxud mulkiy yo‘sindagi harakatlar sodir etishni talab qilish yoxud jabrlanuvchini o‘z mulki yoki mulkka bo‘lgan huquqini berishga majbur qiladigan sharoitga solib qo‘yish- - uch yildan besh yilgacha ozodlikni cheklash yoxud uch yildan besh yilgacha ozodlikdan mahrum qilish bilan; - besh yildan o‘n yilgacha ozodlikdan mahrum qilish bilan; - o‘n yildan o‘n besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi. O‘zbekiston Respublikasi Jinoyat kodeksning 166-moddasiga ko‘ra: Talonchilik, ya’ni o‘zganing mulkini ochiqdan-ochiq talon-toroj qilish- - uch yilgacha axloq tuzatish ishlari yoki ikki yildan besh yilgacha ozodlikni cheklash yoki besh yilgacha ozodlikdan mahrum qilish bilan; - uch yildan besh yilgacha ozodlikni cheklash yoxud uch yildan besh yilgacha ozodlikdan mahrum qilish bilan; - besh yildan o‘n yilgacha ozodlikdan mahrum qilish bilan; - o‘n yildan o‘n besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi. Shuni alohida ta’kidlash kerakki, banklar va boshqa kredit muassasalaridan onlayn shaklda kredit (mikroqarz) mablag‘larini olish maqsadida aldov yoki ishonchni suiiste’mol qilish yo‘li orqali o‘zga shaxsga tegishli bo‘lgan maxsus identifikatsiya talab qiluvchi texnik vositalar (kompyuter, noutbuk, telefon, planshet va h.k)ning maxsus kodlaridan yoki o‘zga shaxsning “elektron raqamli imzo”laridan foydalanib, pul mablag‘lari ajratilishiga va kelgusida ushbu pul mablag‘laridan erkin foydalanish imkoniyatini beruvchi hisob-raqamlarga o‘tkazilishiga erishganlik holatlari firibgarlik sifatida baholanishi lozim. O`zbekiston Respublikasi Jinoyat kodeksining 278^3 -moddasida: Kompyuter tizimidan, shuningdek telekommunikatsiya tarmoqlaridan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus vositalarni o‘tkazish maqsadini ko‘zlab tayyorlash yoxud o‘tkazish va tarqatish jinoyati va unga belgilangan javobgarlik masalasi mustahkamalangan. Shu bilan birga, axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib firibgarlik sodir etish (JK 168-moddasi uchinchi qismi “g” bandi) deganda, moliya, bank muassasalari, fondlar va sh.k. larda bo‘lgan mulkni aldov yo‘li bilan kompyuter texnikasi vositalari, aloqa vositasi, planshet yoki boshqa shu kabi texnik qurilmalar yordamida manipulatsiya qilish orqali amalga oshiriladigan talon-toroj tushuniladi. Bunday firibgarlik kompyuter tizimida ishlov beriladigan, tegishli axborot tashuvchilarda saqlanadigan yoki ma’lumotlarni uzatish tarmoqlari bo‘yicha beriladigan axborotni o‘zgartirish yo‘li bilan ham, kompyuter tizimiga yolg‘on axborot kiritish yo‘li bilan ham sodir etilishi mumkin.

Axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilgan firibgarlik jinoyatini qonunga xilof ravishda (ruxsatsiz) axborot tizimiga kirib yoki undan foydalanib sodir etilgan o‘g‘irlik jinoyatidan farqlashda shuni nazarda tutish lozimki, firibgarlikda jabrlanuvchi aldov yoki ishonchi suiiste’mol qilinishi oqibatida mulkini yoki unga bo‘lgan huquqni axborot texnologiyalaridan foydalanib aybdor egaligiga ixtiyoriy ravishda o‘tkazadi, bunda mulk o‘z egaligidan chiqib ketayotganligini jabrlanuvchi anglagan bo‘lishi kerak. Agar shaxs kompyuter texnikasi yordamida qalbaki hujjat tayyorlab, so‘ngra undan mulkni qo‘lga kiritish uchun foydalangan bo‘lsa, qilmishni JK 168-moddasi uchinchi qismi “g” bandi bilan kvalifikatsiya qilib bo‘lmaydi. Shuningdek, Jinoyat kodeksining 169-moddasida ko‘ra: O‘g‘rilik, ya’ni o‘zganing mol-mulkini yashirin ravishda talon-toroj qilish-agar qonunga xilof ravishda (ruxsatsiz) axborot tizimiga kirib yoki undan foydalanib sodir

etilgan bo‘lsa, besh yildan sakkiz yilgacha ozodlikdan mahrum qilish bilan jazolanadi. Bunday jinoyat sodir etish kiberjinoyat hisoblanadi. Chunki jinoyatchi ushbu jinoyatni axborort vositalaridan foydalangan holda sodir etmoqda. Guvohi bo‘lganimizdek, qonunchiligimizda kibermakon-raqamli makonda sodir etilgan jinoyatlar aksariya hollarda kundalik hayotda sodir etilgan jinoyatlar bilan bir xilda kvalifikatsiya qilinishini taqazo etmoqda. Biroq bir jihatni esda tutish kerakki, kibermuhitda sodir etilayotgan aksariyat jinoyatlar jinoyat sodir etganlik uchun javovgarlik belgilangan yoshga yetmagan shaxslar tomonidan sodir etilmoqda bu esa, jinoyat qonunchiligining majburlash hamda tarbiyalash funksiyalarining to‘g‘ri va maqsadli ishlamasligini keltirib chiqaradi. O‘zbekiston Respublikasi Jinoyat kodeksining 278^3-moddasida: Kompyuter tizimidan, shuningdek telekommunikatsiya tarmoqlaridan qonunga xilof ravishda (ruxsatsiz) 85 foydalanish uchun maxsus vositalarni o‘tkazish maqsadini ko‘zlab tayyorlash yoxud o‘tkazish va tarqatish jinoyati va unga belgilangan javobgarlik masalasi mustahkamalangan.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. https://www.demandsage.com/telegramstatistics.
2. https://t.me/lobushkin/
3. O‘zbekiston Respublikasining jinoyat kodeksi. O‘zbekiston Respublikasi Oliy Kengashining Axborotnomasi, 1995-y., 1-son// https://lex.uz/docs/-111453#-271724.
4. O‘zbekiston Respublikasining Qonuni , 15.04.2022 yildagi O‘RQ-764-son, Qonunchilik ma’lumotlari milliy bazasi, 16.04.2022-y., 03/22/764/0313-son// https://lex.uz/uz/docs/- 5960604.
5. O‘zbekiston Respublikasi Jinoyat kodeksi.
6. O‘zbekiston Respublikasi Oliy sudi Plenumining 2023-yil 23-iyundagi 17-sonli “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi qarorining 9, 22-bandlari.// https://lex.uz/docs/-6523582?ONDATE=23.06.2023%2000#-6523785

KIBERJINOYATCHILIKDA MUHANDISLIK USULIDAN FOYDALANISH

A.A.Abdiraximov

IIV Malaka oshirish instituti Axborot texnologiyalari sikli o‘qituvchisi

e-mail: amr.herezen28@gmail.com tel:+998944282802

Annotatsiya: Ushbu maqolada kiberjinoyatchilikda uchraydigan muhandislik texnik muammolari, jumladan, IOT qurilmalarining zaifligi, kriptografik texnologiyalarning noto‘g‘ri qo‘llanilishi va apparat vositalaridagi xavfsizlik muammolari muhokama qilinadi. Shuningdek, muhandislik nuqtai nazaridan kiberxavfsizlikni ta’minlash bo‘yicha yechimlar, masalan, apparat xavfsizligini mustahkamlash, IOT qurilmalarini yaxshilash va tarmoq himoya mexanizmlarini rivojlantirish bo‘yicha takliflar beriladi. Ushbu yondashuv kiberjinoyatchilikka qarshi samarali kurashish imkonini beradi. Kiiberjinoyatchilikka doir statistik ma’lumotlar diagrammalarda namoyon qilingan.

Kalit so‘zlar: Kiberjinoyatchilik, IOT xavfsizligi, muhandislik muammolari, sun’iy intellekt, kiberxavfsizlik yechimlari.

Kiberjinoyatchilik – bu zamonaviy texnologiyalardan foydalangan holda sodir etiladigan jinoyatlarning bir ko‘rinishi bo‘lib, asosan axborot va kommunikatsiya tizimlariga qaratilgan xatti-harakatlarni o‘z ichiga oladi. Ushbu sohada muhandislik texnikasiga tegishli bir qator muammolar paydo bo‘lmoqda, ular asosan axborot xavfsizligini ta’minlash va hujumlarning oldini olish bilan bog‘liq. [1]

Kiberjinoyatchilik hozirgi kunda jamiyat, biznes va davlat uchun eng jiddiy muammolardan biriga aylanmoqda. Ushbu turdagi muammolarni ishlab chiqarish va texnik vositalar orqali aniqlash va samarali hal qilish mumkin. Muhandislik sharoiti kiberxfsizlikni ta’minlash va zarur-xatarlarni saqlab qolishda muhim narsa ega.

Muhandislik usuli – muammoni tizimli ravishda o‘rganish, tahlil qilish va texnologik yechimlarni ishlab chiqishni o‘z ichiga oladi. Kiberjinoyatchilar bu usuldan axborot tizimlarining zaif tomonlarini o‘rganish, hujumni rejalashtirish va amalga oshirishda foydalanadi.

Kiberjinoyatchilikning muhandislikka ta’siri:

Kiberjinoyatchilik nafaqat dasturiy ta’minot, balki apparat va muhandislik tizimlariga ham ta’sir ko‘rsatadi. Quyida asosiy muammolarni keltirib o‘tamiz:

Ijtimoiy muhandislik – inson omilidan foydalanib, tizimlarga noqonuniy kirish usuli. Bu usul foydalanuvchilarni manipulyatsiya qilish orqali parollarni yoki shaxsiy ma‘lumotlarni olishni maqsad qiladi.

IOT qurilmalarining zaifligi: Internetga ulangan qurilmalarning xavfsizlik standartlari past bo‘lgani sababli ularga hujum qilish osonlashmoqda. Bu tizim dizaynida muhandislik xatolariga yo‘l qo‘yilishidan kelib chiqadi.

Iso 27001 ning asosiy tushunchasi bo‘lgan axborot xavfsizligini boshqarish tizimi, tashkilot va tashkilotlarning uzluksizligini ta’minlashga qaratilgan va qo‘llab-quvvatlaydigan eng asosiy qiymatdir. Agar bir nechta aktiv yo'qolgan bo‘lsa, etishmovchilikni bartaraf etish mumkin bo‘lgan holatlar mavjud, yo‘qolgan ma’lumotlarning moddiy ekvivalenti mumkin emas. Buning sababi o‘zgarishlarning uzluksiz o‘zaro ta’siri va bugungi rivojlanayotgan sharoitda axborotning ahamiyati va ahamiyati tobora ortib borayotgan shaxsga aylanib bormoqda. [2]

Kelgusida kiber jinoyatchilar xavfsizlik tizimlarini mustaqil ravishda o‘rgana oladigan sun’iy intellektdan foydalanishni boshlaydilar. 2024-yilga kelib, kiber jinoyatlardan moliyaviy yo‘qotishlar deyarli ***70% ga*** etadi. Juniper Research tadqiqotchilarining fikriga ko‘ra, zarar har yili o‘rtacha ***11 foizga oshadi***.

2024-yilga kelib 5 trillion dollardan oshadi. O‘tgan yili mutaxassislar kiber jinoyatlardan etkazilgan zararni 3 trillion dollarga baholashgan. Har yili kompaniyalar tobora ko‘proq raqamli muhitga bog‘liq bo‘lib, zarar etkazilishi ma’lumotlarning tarqalishi uchun qonun bo‘yicha olinadigan jarimalar tufayli ortadi. Vaqt o‘tishi bilan nafaqat himoya usullari yaxshilanmoqda. Tahlilchilar kiber jinoyatchilar kelajakda xavfsizlik tizimlarini mustaqil o‘rganishga qodir bo‘lgan sun’iy intellektdan foydalanishni boshlashlari haqida ogohlantirmoqda.

So‘nggi yillarda IT texnologiyasi kiber tahdidlardan himoya qilish uchun faol foydalanilmoqda. Kiberxavfsizlik korporativ madaniyatning tobora muhim qismiga aylanib bormoqda, ammo bu tendentsiya kompyuter tizimlari foydalanuvchilari

orasida keng tarqalmadi. Xodimlarni kiberxavfsizlik asoslariga o‘rgatish ushbu sohada xarajatlarni yanada samarali rejalashtirishga yordam beradi, tahlilchilar fikriga ko‘ra, har yili atigi 8 foizga o‘sadi. Mutaxassislar, shuningdek, IT-kompaniyalar har doim inson omilini hisobga olishlari kerakligini ta’kidladilar, chunki tajovuzkorlar ijtimoiy muhandislik usullaridan faol foydalanishda davom etmoqdalar.

Xulosa.

Kiberjinoyatchilikning texnik muammolari muhandislik sohasidagi zaifliklar bilan bevosita bog‘liq. Bu muammolarni hal qilish uchun zamonaviy texnologiyalarni joriy etish, kuchli xavfsizlik tizimlarini loyihalash va global hamkorlikka asoslangan yondashuv zarur. Kiberxavfsizlikni ta’minlash nafaqat dasturiy ta’minot, balki muhandislik texnologiyalari sohasidagi yutuqlar bilan ham bog‘liq.

Adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasining Prezidenti Sh. MIRZIYOYEV ning 2022-yil 15-apreldagi, O‘RQ-764-son Qonuni.
2. ISO/IEC 27001: Axborot xavfsizligini boshqarish.
3. “The Art of Cyberwarfare: An Investigator’s Guide to Espionage, Ransomware, and Organized Cybercrime” – Jon DiMaggio.
4. https://natalinawtonia.pages.dev/
5. https://www.securitylab.ru/news/500645.php

KIBERJINOYATCHILIKKA QARSHI KURASHISHDA SUN’IY INTELLEKT VA HUQUQIY TEXNOLOGIYALARNING INTEGRATSIYASI

Burxonov Bahodir Hayotovich

O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti Jismoniy tayyorgarlik sikli o‘qituvchisi
bahodirburxonov87@gmail.com

Annotatsiya: Ushbu maqolada kiberjinoyatchilikka qarshi kurashda sun’iy intellekt (SI) va huquqiy texnologiyalarning o‘zaro integratsiyasi masalalari ko‘rib chiqiladi. Kiberjinoyatlar sonining oshib borishi global miqyosda iqtisodiy, ijtimoiy va huquqiy muammolarni keltirib chiqaradi. Tadqiqotda SI texnologiyalarining huquqni muhofaza qilish organlari va yuridik tizimda qo‘llanilishi, shuningdek, huquqiy texnologiyalarning kiberxavfsizlik sohasidagi roli tahlil qilinadi. Maqolada keltirilgan statistik ma’lumotlar va tahlillar asosida kiberjinoyatchilikka qarshi kurash samaradorligini oshirish bo‘yicha tavsiyalar beriladi.

Kalit so‘zlar: Kiberjinoyatchilik, sun'iy intellekt, huquqiy texnologiyalar, kiberxavfsizlik, blokcheyn, mashinani o‘rganish, raqamli dalillar, LegalTech.

ИНТЕГРАЦИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ПРАВОВЫХ ТЕХНОЛОГИЙ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Бурхонов Баходир Хаётович

Преподаватель цикла физической подготовки Институт повышения квалификации Министерство внутренних дел Республики Узбекистан
bahodirburxonov87@gmail.com

Аннотация: В данной статье рассматриваются вопросы интеграции искусственного интеллекта (ИИ) и правовых технологий в борьбе с киберпреступностью. Рост числа киберпреступлений приводит к экономическим, социальным и правовым проблемам на глобальном уровне. В исследовании анализируется применение технологий ИИ в правоохранительных органах и судебной системе, а также роль правовых технологий в области кибербезопасности. На основании приведённых статистических данных и анализов в статье даны рекомендации по повышению эффективности борьбы с киберпреступностью.

Ключевые слова: Киберпреступность, искусственный интеллект, правовые технологии, кибербезопасность, блокчейн, машинное обучение, цифровые доказательства, LegalTech.

INTEGRATION OF ARTIFICIAL INTELLIGENCE AND LEGAL TECHNOLOGIES IN COMBATING CYBERCRIME

Burkhonov Bahodir Hayotovich

Teacher of physical training cycle Institute of advanced training Ministry of Internal Affairs of the Republic of Uzbekistan
bahodirburxonov87@gmail.com

Abstract: This article examines the integration of artificial intelligence (AI) and legal technologies in combating cybercrime. The increasing number of cybercrimes is causing economic, social, and legal challenges on a global scale. The study analyzes the application of AI technologies in law enforcement agencies and judicial systems, as well as the role of legal technologies in cybersecurity. Based on the provided statistical data and analyses, the article offers recommendations for enhancing the effectiveness of the fight against cybercrime.

Keywords: Cybercrime, artificial intelligence, legal technologies, cybersecurity, blockchain, machine learning, digital evidence, LegalTech.

Kirish. Kiberjinoyatchilik zamonaviy dunyoda eng dolzarb muammolardan biriga aylangan. 2023-yilgi statistik ma’lumotlarga ko‘ra, dunyo bo‘ylab kiberjinoyatlar tufayli iqtisodiy zarar **$8,4 trillion AQSh dollarini** tashkil etdi va bu ko‘rsatkich 2025-yilga kelib **$10,5 trillion** ga yetishi prognoz qilinmoqda (Cybersecurity Ventures, 2023). Shu bilan birga, kiberhujumlar soni har yili o‘rtacha **15%** ga oshmoqda. Bunday sharoitda kiberjinoyatchilikka qarshi samarali kurashish

uchun sun’iy intellekt (SI) va huquqiy texnologiyalarni (LegalTech) integratsiya qilish dolzarb masalaga aylandi.

Kiberjinoyatchilik va uning oqibatlari

Ma’lumotlarni o‘g‘irlash va shaxsiy ma’lumotlarga noqonuniy kirish: 2022-yilda dunyo bo‘ylab 22 milliarddan ortiq ma’lumotlar bazasi buzilgan (Statista, 2023).

Moliyaviy firibgarliklar: 2023-yilda moliyaviy tashkilotlarga qaratilgan kiberhujumlar soni 38% ga oshgan.

DDoS (Distributed Denial of Service) hujumlari: Internet infratuzilmasiga qaratilgan bunday hujumlar 2023-yilda o‘rtacha har 3 soniyada bir marta amalga oshirilgan.

Ransomware (talabnoma dasturlar): Har 10 soniyada bir korxona ransomware hujumiga uchragan va bu holatlar global iqtisodiyotga **$20 milliard** zarar keltirgan.

Oqibatlari:

- *Iqtisodiy zararlar:* Moliyaviy yo‘qotishlar, jarimalar va sud xarajatlari.
- *Ijtimoiy xavf-xatarlar:* Shaxsiy hayotning buzilishi, ishonchning pasayishi.
- *Xavfsizlikka tahdidlar:* Milliy va korporativ darajadagi xavfsizlikka salbiy ta’sir.

Sun’iy intellektning kiberjinoyatchilikka qarshi kurashdagi roli.

Sun’iy intellekt texnologiyalari kiberjinoyatchilikni aniqlash, oldini olish va tekshirish jarayonlarini avtomatlashtirishda keng qo‘llanilmoqda. Quyida SI’ning asosiy qo‘llanilish yo‘nalishlari ko‘rsatilgan:

1. **Kiberxavfsizlikdagi SI algoritmlari.**

- *Xavflarni aniqlash:* SI algoritmlari real vaqt rejimida kiberhujumlarni tahlil qiladi va ularni aniqlashda insonning xatosizligini oshiradi. Masalan, 2023-yilda SI yordamida 94% kiberhujumlar avtomatik ravishda aniqlangan (Gartner, 2023).
- *Tahdidlarni prognoz qilish:* Mashinani o‘rganish texnologiyalari tahdidlarning oldindan prognoz qilinishida samaradorlikni 85% ga oshiradi.

2. **Blokcheyn va SI integratsiyasi.**

Blokcheyn texnologiyasi SI bilan birgalikda ma’lumotlarning yaxlitligini ta’minlaydi va tranzaksiyalarni kuzatib borishda aniqlikni oshiradi. 2023-yilda blokcheyn asosidagi kiberxavfsizlik platformalari kiberjinoyatlar sonini 30% ga kamaytirishga yordam berdi.

3. **Avtomatlashtirilgan monitoring tizimlari.**

Huquqni muhofaza qilish organlari SI asosidagi monitoring tizimlaridan foydalanib, kiberjinoyatchilar faoliyatini kuzatadi va noqonuniy faoliyatni real vaqt rejimida aniqlaydi.

Huquqiy texnologiyalarning roli.

Huquqiy texnologiyalar (Legal Tech) kiberjinoyatlarga qarshi kurashda quyidagi yo‘nalishlarda qo‘llaniladi:

Raqamli dalillarni yig‘ish va tahlil qilish: Kiberjinoyatlar bo‘yicha dalillarni yig‘ish va ularni tahlil qilishda huquqiy texnologiyalar muhim ahamiyat kasb etadi. Raqamli dalillarni avtomatik tahlil qilish tizimlari inson ishtirokisiz dalillarni qayta ishlashda katta tezlik va aniqlikni ta’minlaydi. 2023-yilda LegalTech platformalari orqali 70% kiberjinoyat ishlarida dalillar muvaffaqiyatli yig‘ilgan.

Smart-kontraktlar va yuridik jarayonlarni avtomatlashtirish: Blokcheyn asosidagi smart-kontraktlar qonuniy jarayonlarni avtomatlashtirishda yordam beradi va firibgarlik holatlarini kamaytiradi. Bu texnologiyalar kelishuvlar bajarilishini kafolatlab, kiberjinoyatchilarni qonuniy javobgarlikka tortish imkonini oshiradi.

Kiberjinoyatchilikka oid qonunchilikni avtomatlashtirish: Legal Tech algoritmlari kiberjinoyatchilikka oid qonunchilikni avtomatik ravishda tahlil qiladi va qonunchilikdagi bo‘shliqlarni aniqlashga yordam beradi. Masalan, AI-Powered Legal Solutions platformalari 2023-yilda kiberjinoyatlar bo‘yicha sud qarorlarining 90% aniqligini ta’minlagan.

Statistik natijalar va tavsiyalar:

- 2023-yilda SI va Legal Tech integratsiyasi yordamida global kiberjinoyatlar soni 15% ga kamaytirildi.
- SI asosidagi kiberxavfsizlik tizimlari hujumlarni aniqlash samaradorligini 94% ga oshirdi.
- Blokcheyn texnologiyalari kiberjinoyatlar bo‘yicha tranzaksiyalarni kuzatishda aniqlikni 85% ga yetkazdi.

Tavsiyalar:

- *SI va LegalTech’ni keng joriy qilish:* Huquqni muhofaza qilish va sud tizimlarida SI va LegalTech texnologiyalarini kengroq qo‘llash talab etiladi.
- *Xalqaro hamkorlikni kuchaytirish:* Kiberjinoyatchilikka qarshi kurashda xalqaro tashkilotlar bilan texnologik hamkorlikni yo‘lga qo‘yish muhim.
- *Kiberxavfsizlik bo‘yicha huquqiy bazani mustahkamlash:* Kiberjinoyatlarga doir qonunchilikni zamonaviy texnologiyalar talablariga mos ravishda yangilash lozim.
- *Malakali mutaxassislarni tayyorlash:* SI va LegalTech bo‘yicha maxsus malakali kadrlarni tayyorlash strategik ahamiyatga ega.

Kiberjinoyatchilik va unga qarshi kurashdagi texnologiyalarning samaradorligini aks ettiruvchi jadval.

Ko‘rsatkich	Miqdor/Prosent	Manba/Izoh
Kiberjinoyatchilikdan global iqtisodiy zarar	$8,4 trillion (2023), $10,5 trillion (2025)	Cybersecurity Ventures, 2023
Kiberhujumlarning yillik o‘sish darajasi	15%	Statista, 2023
Talabnoma dasturlari (ransomware) hujumlari	Har 10 soniyada 1	Gartner, 2023
Kiberjinoyatlarga uchragan ma’lumotlar bazasi	22 milliard (2022)	Statista, 2023
Kiberxavfsizlikka SI qo‘llanilishi samaradorligi	94% kiberhujumlarni aniqlash	Gartner, 2023

Mashinani o‘rganish yordamida tahdidni prognozlash	85% samaradorlik	Cybersecurity Ventures, 2023
Blokcheyn asosidagi xavfsizlik platformalari	Kiberjinoyatlar sonini 30% ga kamaytirgan	Blokcheyn texnologiyalari tadqiqot markazi, 2023
LegalTech yordamida dalillar yig‘ish samaradorligi	70% muvaffaqiyat	LegalTech platformalari, 2023
Kiberjinoyatlar bo‘yicha sud qarorlarining aniqligi	90%	AI-Powered Legal Solutions, 2023

Ushbu jadval kiberjinoyatchilikning global miqyosdagi jiddiyligi va unga qarshi kurashda sun’iy intellekt va huquqiy texnologiyalarning samaradorligini ko‘rsatadi. Raqamlar asosida kiberjinoyatchilikka qarshi strategiyalarni rejalashtirishda ushbu ma'lumotlardan foydalanish mumkin.

Xulosa. Kiberjinoyatchilikka qarshi kurashda sun'iy intellekt va huquqiy texnologiyalarning integratsiyasi zamonaviy texnologik yondashuvlarni talab qiladi. SI va LegalTech nafaqat kiberjinoyatlarni aniqlash va ularga qarshi kurashish samaradorligini oshiradi, balki huquqiy jarayonlarni avtomatlashtirib, vaqt va resurslarni tejashga ham xizmat qiladi. Kelgusida ushbu texnologiyalarni rivojlantirish va ularni qo‘llash doirasini kengaytirish orqali kiberjinoyatchilikka qarshi kurashda yanada yuqori natijalarga erishish mumkin.

ADABIYOTLAR:

1. Cybersecurity Ventures. “Cybercrime Report 2023”. (2023).
2. Statista. “Cybersecurity Statistics”. (2023).
3. Gartner. “AI in Cybersecurity: Annual Report”. (2023).
4. Blokcheyn texnologiyalari bo‘yicha xalqaro tadqiqotlar markazi. (2023).

КИБЕРЖИНОЯТЧИЛИККА ҚАРШИ КИБЕР МАДАНИЯТНИ РИВОЖЛАНТИРИШ

Бейсенов Кенжабай Сарсанбаевич,

Малака ошириш институти Касбий тайёргарлик факультети Махсус фанлар цикли ўқитувчиси

Хожибеков Зиёмиддин Насриддинович

Малака ошириш институти Касбий тайёргарлик факультети Махсус фанлар катта цикли ўқитувчиси

Аннотация: Мазкур мақолада кибержиноятчиликка қарши кибер маданиятни ривожлантириш бўйича илмий асосланган таклиф ва тавсиялар берилган.

Аннотация: в данной статье представлены научно обоснованные предложения и рекомендации по развитию киберкультуры, направленной против киберпреступности.

Annotation: this article provides scientifically based proposals and recommendations for the development of cyberculture against cybercrime.

Таянч сўзлар: Киберхавфсизлик, кибержиноятчилик, киберхавфсизлик объекти, киберҳужум, кибертаҳдид, интернет.

Ключевые слова: кибербезопасность, киберпреступность, объект кибербезопасности, кибератака, кибератака в Интернете.

Base words: cybersecurity, cybercrime, cybersecurity object, cyberattack, cyberattack, internet.

Кибержиноятчиликка қарши курашда энг мураккаб муаммолардан бири ушбу турдаги жиноятларнинг виртуал муҳитда ва исталган ҳудуддан содир этилиши имкониятининг мавжудлиги ҳисобланади. Аксарият ҳолларда, ташқи хавфлар манбаи Ўзбекистон Республикаси қонунчилиги юрисдикцияси доирасига кирмайди. Бу эса, ҳуқуқий чоралар тизимини қўллашни муайян даражада мураккаблаштиради. Кибержиноятчилар, одатда, миллий чегараларни четлаб ўтган ҳолда, жаҳон тармоғига уланган ҳар қандай компьютерга, электрон дастурга ҳужум қилади. Ёки гўё бошқа манбалар ёхуд бундай хатти-ҳаракатлар жиноят ҳисобланмайдиган мамлакатдан туриб шундай хужумни амалга оширади. Бу эса, ўз навбатида, қатор ҳуқуқий зиддиятларни келтириб чиқармоқда.

Кибержиноятчиликка қарши кибер маданиятни ривожлантиришга тўхталишдан олдин, қуйидаги тушунчаларга таъриф бериб ўтиш мақсадга мувофиқдир: **кибертаҳдид** — кибермаконда шахс, жамият ва давлат манфаатларига таҳдид солувчи шарт-шароитлар ва омиллар мажмуи; **киберхавфсизлик** — кибермаконда шахс, жамият ва давлат манфаатларининг ташқи ва ички таҳдидлардан ҳимояланганлик ҳолати; **киберхавфсизлик объекти** — ахборотнинг киберҳимоя қилинишини ҳамда миллий ахборот тизимлари ва ресурсларининг киберхавфсизлигини таъминлашга доир фаолиятда фойдаланиладиган ахборот тизимлари мажмуи, шу жумладан муҳим ахборот инфратузилмаси объектлари; **киберхавфсизлик субъекти** — миллий ахборот ресурсларига эга бўлиш, улардан фойдаланиш ва уларни тасарруф этиш ҳамда улардан фойдаланиш бўйича электрон ахборот хизматлари кўрсатиш, ахборотни ҳимоя қилиш ҳамда киберхавфсизлик билан боғлиқ муайян ҳуқуқлар ва мажбуриятларга эга бўлган юридик шахс ва (ёки) якка тартибдаги тадбиркор, шу жумладан муҳим ахборот инфратузилмаси субъектлари; **киберҳимоя** — киберхавфсизлик ҳодисаларининг олдини олишга, киберҳужумларни аниқлашга ва улардан ҳимоя қилишга, киберҳужумларнинг оқибатларини бартараф этишга, телекоммуникация тармоқлари, ахборот тизимлари ҳамда ресурслари фаолиятининг барқарорлигини ва ишончлилигини тиклашга қаратилган

ҳуқуқий, ташкилий, молиявий-иқтисодий, муҳандислик-техник чора-тадбирлар, шунингдек маълумотларни криптографик ва техник жиҳатдан ҳимоя қилиш чора-тадбирлари мажмуи; **киберҳужум** — кибермаконда аппарат, аппарат-дастурий ва дастурий воситалардан фойдаланган ҳолда қасддан амалга ошириладиган, киберхавфсизликка таҳдид соладиган ҳаракат[27]; **маданият** — жамият, инсон ижодий куч ва қобилиятлари тарихий тараққиётининг муайян даражаси. Кишилар ҳаёти ва фаолиятининг турли кўринишларида, шунингдек, улар яратадиган моддий ва маънавий бойликларда ифодаланади[28].

Бундай жиноят тури глобаллашиб бораётгани эътиборга олинадиган бўлса, бугун ҳеч қайси мамлакат ушбу хавфга нисбатан мустақил равишда бир ўзи қаршилик кўрсата олмайди. Бундай шароитда халқаро ҳамкорликни кенгайтириш, кибержиноятчиликка қарши биргаликда ҳаракат қилиш ва уни текшириш борасида тегишли органлар фаолиятини тартибга солиш ҳамда ўзаро ҳамкорликнинг халқаро ҳуқуқий механизмларини ишлаб чиқиш ягона йўлдир[29]. Шу сабабдан, кибержиноятчилик муаммоси жаҳон ҳамжамиятини унга қарши курашиш юзасидан зарур чоралар кўришга ундамоқда.

Бугунги кунда Республикамизда фуқароларнинг ахборотни эркин излаш ва олишга доир конституциявий ҳуқуқларини амалга ошириш, ахборот-коммуникация технологияларини кенг жорий қилиш мақсадида бир қатор ташкилий тадбирлар амалга оширилмоқдалар.

Хусусан, Ўзбекистон Республикаси Ички ишлар вазирлиги Тезкор-қидирув департаментида Киберхавфсизлик маркази ташкил этилиб, масъул ходимлар томонидан киберхавфсизлик қоидаларига риоя қилиш, ҳозирги кунда учраётган кибертаҳдидлар, интернет тармоғидаги ҳуқуқбузарликлар ва улардан ҳимояланиш бўйича тегишли кўрсатма ва тавсиялар бериб келинмоқда.

Ўз навбатида, ҳозирги кунда авж олиб бораётган онлайн қимор ва таваккалчиликка асосланган ўйинлар, Интернет тармоғидаги “молиявий пирамида”лар, уларнинг қонун билан тақиқланганлиги ҳамда жамиятга зарарлари, кибержиноятларнинг ўзига хос хусусиятлари, ёлғон ахборотларни тарқатганлик учун жавобгарликнинг муқаррарлиги бўйича тушунтириш ишлари ҳар бир ички ишлар органлари ва мутасадди ташкилотлар билан ҳамкорликда аҳолига кенг тарғиб қилиб келинмоқдалар.

Бу борада Ички ишлар органлари ҳар бир соҳа хизмат ходимлари томонидан Кибермаданиятни юксалтириш доирасида барча ташкилот ва идораларда, аҳоли кўп тўпланадиган жамоат жойларида ижтимоий тармоқлардаги ёлғон хабарларга ишониб, кибержиноят қурбони бўлиб қолишларининг олдини олишга қаратилган тарғибот тадбирлари ўтказилмоқда.

Қолаверса, “Мобиль тарғибот” гуруҳи ходимлари томонидан туманлар ҳудудида “маҳаллабай” ва “хонадонбай” тарзда фуқароларнинг банк пластик карталари ва шахсига доир маълумотларини сир сақлашлари лозимлиги

[27] https://lex.uz/docs/5960604
[28] https://qomus.info/encyclopedia/cat-m/madaniyat-uz/
[29] Тожиев С. Кибержиноятчилик – шахс ва жамият хавфсизлигига таҳдид. // www.uza.uz

уқтирилиб, ижтимоий тармоқлардаги фирибгарларнинг тузоғига тушиб қолишларининг олдини олиш бўйича огоҳликка чорловчи тарғибот тадбирлари амалга ошириб келинмоқда.

Шу ўринда кибермаданият, фуқаролар турли фирибгарлар тузоғига тушмаслиги учун зарурий чоралар ҳақида айрим фикрларга тўхталиб ўтадиган бўлсак.

Кибермаданият — бу одамларнинг интернет ва бошқа рақамли технологиялар орқали ўзаро муносабатларини ташкил қилиш усуллари ва қоидаларининг мажмуидир.

Бу тушунча, одатда, қуйидаги жиҳатларни ўз ичига олади: жумладан, интернетда ёзиш, мулоқот қилиш ва ўзини тутиш қоидалари. Бу, хусусан, мулойим ва ҳурматли бўлиш, қўпол сўзлардан фойдаланмаслик, спам жўнатмаслик ва бошқа фойдаланувчилар билан муносабатларда адолатли бўлиш лозим деганидир; фуқароларнинг шахсий маълумотларини ҳимоя қилиш, кучли пароллар ишлатиш, хавфсизлик бўйича маслаҳатларни билиш ва уларга риоя қилиш ҳар қачонгидан муҳимдир; онлайн шахсий ҳаётни сақлаш, шахсий маълумотларни номаълум ёки ишончсиз манбалар билан баҳам кўрмаслик. Ишончли ва тасдиқланган маълумот манбаларидан фойдаланиш, ёлғон ёки нотўғри маълумотларни тарқатмаслик лозим бўлади; ижтимоий тармоқларда мулоқот қилиш қоидалари, масалан, бошқаларнинг шахсий ҳаётига ҳурмат, фотосуратларни ва бошқа материалларни рухсатсиз тарқатмаслик кибермаданиятнинг бир қисми ҳисобланади.

Кибермаданиятнинг ривожланиши учун фуқаролар бу қоидаларни билиши ва уларга риоя қилиши шарт. Бу жамиятдаги ҳамкорлик ва ишонч муҳитини яратишга ёрдам беради ва интернетдаги хавфсизлик даражасини оширади. Кибермаданиятнинг ўзига хос жиҳатлари болалар ва ўсмирлар орасида ҳам муҳим аҳамиятга эга бўлиб, уларни интернетдан хавфсиз ва масъулиятли фойдаланишга ўргатади.

Кибермаданиятни аҳоли орасида кенг ёйиш жамиятда интернет ва рақамли технологиялардан масъулиятли ва хавфсиз фойдаланишни таъминлаш учун муҳим аҳамиятга эга.

Том маънода жамият бугунги кунда ахборот маконида кўплаб маълумотларга эга бўлмоқда. Уларда ахборотларни саралаш имконияти йўқ. Интернет жаҳон ахборот тармоғидан фойдаланишда, албатта, ўта эҳтиёткорлик талаб этилади.

Зеро, инсонлар ишончига кираётган айрим фирибгарлар содда одамларни алдаган ҳолда, уларнинг ҳисобларидаги мавжуд маблағларни алдов йўли билан эгаллаб олмоқдалар.

Интернет тармоғларидаги ҳуқуқбузарликларга қарши курашиш биргина ҳуқуқни муҳофаза қилувчи органларнинг вазифаси бўлиб қолмасдан, балки, бутун жамиятимизнинг иши эканлиги, кибержиноятларга қарши курашишда уларнинг фаол қатнашишлари мақсадга мувофиқ эканлигини эслатиб ўтмоқчимиз.

Бу борада туманлардаги барча сектор раҳбарлари, мутасадди ташкилот ва идоралар билан ҳамкорликда аниқ белгиланган чора-тадбирлар асосида комплекс тарғибот-ташвиқот тадбирлари давом эттирилиши керак[30].

Жиноятни фош қилишдан кўра, уни олдини олиш учун, кибержиноятларга қарши курашишни тарғиб қилувчи, ҳамда кибержиноятлардан огоҳ бўлишга қаратилган инновацион ёндашув асосида маҳалла, катта ёшдаги аҳоли вакиллари ва блогерлар ўртасида "Энг яхши маҳалла", "Банк картаси кодини ҳеч кимга бермайман", "Энг яхши контент", "Энг яхши монолог" каби танловлар ҳам ўтказиш мақсадга мувофиқдир. Ниятимиз аҳолининг кибержиноятларга қарши иммунитетини ошириш, интернет тармоқларидаги фирибгарларнинг алдовига осонгина чув тушмаслик ҳолатларининг олдини олишдан иборатдир[31].

Аҳолини янада огоҳликка чақириш мақсадида ушбу тарғибот тадбирлари маҳаллабай, хонадонбай ва фуқаробай шаклда аҳолининг ҳар бир қатлами ўртасида олиб бориш керак.

Фойдаланилган адабиётлар рўйхати

1. Ўзбекистон Республикасининг Конституцияси. – Т., 2023й.
2. Мирзиёев Ш.М. Миллий тараққиёт йўлимизни қатъият билан давом эттириб, янги босқичга кўтарамиз. – Тошкент: “Ўзбекистон”, И жилд. НМИУ, 2017, – 592 б.
3. Ўзбекистон Республикасининг 2022 йил 15 апрелдаги “ Киберхавфсизлик тўғрисида”ги ЎРҚ-764-сон Қонуни.
4. Тожиев С. Кибержиноятчилик – шахс ва жамият хавфсизлигига таҳдид. // www.uza.uz.
5. https://uzhurriyat.uz/2024/07/17/kiberjinoyatchilikka-qarshi-kibermadaniyat/?ysclid=m43yyj3upm702612031.
6. https://lex.uz/docs/5960604.
7. https://qomus.info/encyclopedia/cat-m/madaniyat-uz/

КИБЕРЖИНОЯТ ТУШУНЧАСИ ВА УНИНГ ЎЗИГА ХОС БЕЛГИЛАРИ

Б.Б.Умурзоқов

Ўзбекистон Республикаси ИИВ Малака оширш институти Жанговар тайёргарлик цикли катта ўқитувчиси

Аннотация: Мазкур мақолада ахборот маконини ўзлаштириш технологияси, “кибер жиноят” ва “компьютер жинояти” атамаси, Facebook, Microsoft, Twitter ва YouTube хусусий компаниялари кибер терроризмга қарши курашиш мақсадида бирлашиши ҳамда ахборот-коммуникация жабҳасидаги жиноятларнинг мунтазам профилактикасини йўлга қўйиш юзасидан илмий асосланган таклиф ва тавсиялар берилган.

Аннотация: В данной статье рассматриваются технологии освоения информационного пространства, термины «кибер преступление» и

[30] https://uzhurriyat.uz/2024/07/17/kiberjinoyatchilikka-qarshi-kibermadaniyat/?ysclid=m43yyj3upm702612031
[31] https://aviib.uz/uz/news/andizhon-vilotida-tkazil

«компьютерное преступление», а также объединение частных компаний Facebook, Microsoft, Twitter и YouTube для борьбы с кибертерроризмом. Кроме того, представлены научно обоснованные предложения и рекомендации по организации регулярной профилактики преступлений в области информационно-коммуникационных технологий.

Annotation: This article discusses the technologies for mastering the information space, the terms "cyber crime" and "computer crime," as well as the collaboration of private companies such as Facebook, Microsoft, Twitter, and YouTube in the fight against cyber terrorism. Additionally, scientifically based proposals and recommendations are presented for organizing regular prevention of crimes in the field of information and communication technologies.

Калит сўзлар: “Кибер жиноят”, “компьютер жинояти”, “Детерминация”, диалектик детерминизм, “Кибер таҳдидга қарши Кибер мудофаа” ва кибер жиноятчиликнинг қуйидаги фарқловчи белгилар.

Базовые слова: «Кибер преступление», «компьютерное преступление», «детерминация», диалектический детерминизм, «Кибер защита от кибер угроз» и различительные признаки кибер преступности.

Base words: "Cybercrime," "computer crime," "determination," dialectical determinism, "Cyber defense against cyber threats," and distinguishing features of cybercrime.

Маълумки, замонавий дунёни турли хил технологиялардан фойдаланмасдан тасаввур қилиб бўлмайди. сўнгги йилларда “Интернет” ва инсониятнинг ахборот технологиялари соҳаларидаги ихтиролари натижасида Ахборот маконидан фойдаланувчилар сони кундан-кунга ортиб бормоқда ва шу тариқа унинг таъсири доимий равишда кенгаймоқда.

Натижада бутун инсоният сингари жиноят олами ҳам ривожланиб, ахборот технологиялари соҳасини мукаммал ўрганган баъзи бир шахс ёки гуруҳлар жиноят содир этишнинг янги технологияларини ўзлаштирмоқдалар.

Ахборот маконини ўзлаштириш технологиясининг пайдо бўлиши билан жиноятнинг янги тури – кибержиноятлар юзага келди.

Дунё миқиёсида кибержиноятларнинг тарқалиши шахдам қадамлар билан кундан кунга ривожланиб бормоқда. Шу муносабат билан кибержиноятчилик муаммосини тушуниш масалалари замонавий жамиятнинг энг муҳим Кибержиноятлар ҳар бир даврда ахборот-коммуникация технологияларининг ривожи туфайли турлича доктринал ва расмий таърифларга эга.

Кибержиноятнинг вужудга келиши билан тадқиқотчилар ўртасида “кибержиноят” атамаси қанақа бўлиши ва ушбу атама нималарни ўз ичига олиши кераклиги ҳақида мунозаралар пайдо бўлиб, хонузгача давом этиб келмоқда. Тадқиқотчилар ўртасидаги баҳслар давомида “кибер жиноят” ва “компьютер жинояти” атамаларининг комбинацияси масаласини кўтарадиган бир неча назариячилар мавжуд, бу икки тушунча ўртасидаги муносабатлар бўйича биринчи назарияда “кибер жиноят” атамаси “компьютер жинояти”га қараганда кенгроқлигини таъкидлайди.

Ушбу назариянинг вакиллари – рус олимлари В.А.Номоконов ва Т.Л.Тропина ўз тадқиқотдарида “кибержиноят” тушунчасини келтириб чиқарадиган сўзларнинг маъносини тавсифловчи хорижий изоҳли луғатларни таҳлил қилиб, таҳлил натижаларига кўра, “кибержиноят” атамаси “компьютер жинояти”дан кенгроқ деган хулосага келишди[32].

Улар ўз фикрларида ахборот маконида содир этиладиган жиноятларнинг моҳиятини аниқроқ ва тўғри тасвирлайдилар, бундан ташқари, тадқиқот натижаларига кўра, олимлар “кибер жиноят”га ўзларининг таърифларини беришган. Уларнинг фикрича, “кибержиноят - бу компьютер тизимлари ёки компьютер тармоқлари, шунингдек кибермаконга киришнинг бошқа ёрдамида ёки улар орқали кибермаконда, компьютер тизимлари ёки тармоқлари воситалари доирасида ҳамда компьютер тизимларига, компьютер тармоқларига қарши содир этилган хар кандай жиноятлар мажмуидир[33].

Шунингдек Россиянинг бошқа бир гуруҳ олимлари яъни Т.Н. Шарыпова ва А.А.Сидоренко ўз назариясида “кибер жиноят” атамаси “компьютер тизими ёки тармоғи ёрдамида, компьютер тизими ёки тармоғи доирасида, компьютер тизими ёки тармоғига қарши содир этилиши мумкин бўлган ҳар қандай жиноятни” бирлаштирган деб ҳисоблайдилар. “Компьютер жинояти”га қараганда кенгроқ маънога эга деган назарияни энг тўғри деб ҳисоблаш мақсадга мувофиқ бўларди[34].

Ушбу ёндашув вакиллари томонидан берилган таъриф кенгроқ ҳаракатлар доирасини ўз ичига олади ва замонавийлик талабларига яхшироқ жавоб беради.

Кибержиноятнинг моҳиятини яхшироқ тушуниш учун терминологиядан ташқари, ушбу турдаги жиноятларнинг ўзига хос белгиларини ҳам мукаммал ўрганиш керак бўлади.

Бу умумий содир этилган жиноятлардан ахборот макондаги жиноятларни алоҳида тахлилини олиб боришлик учун имконият беради ҳамда кибержиноятларга қарши курашишнинг энг самарали чораларини белгилаб беради.

Кўпгина тадқиқотчилар кибержиноятнинг ўзига хос хусусиятлари бўйича, ўз фикирларини бериб ўтганлар. Жумладан, рус олим И.Г.Чекунов ички ва халқаро ҳуқуқий ҳужжатларни таҳлил қилиш асосида кибержиноятчилигининг нафақат жиноий қилмишларини ўзига хос белгиларининг тавсифи балки жиноятнинг субъектлари, мақсадлари ва жиноятни фош этишдаги мураккабликларини кўрсатиб беради.

Шунингдек Россиянинг бошқа бир гурух олимлари яъни Т.Н. Шарыпова ва А.А.Сидоренко ўз назариясида “кибер жиноят” атамаси “компютер тизими ёки тармоғи ёрдамида, компютер тизими ёки тармоғи доирасида, компютер тизими ёки тармоғига қарши содир этилиши мумкин бўлган ҳар қандай жиноятни” бирлаштирган деб ҳисоблайдилар.

---

[32] https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza.

[33] ITU Toolkit For Cybercrime Legislation. ITU, 2017

[34] Никиташенко, В. В. Понятие и признаки киберпреступности / В. В. Никиташенко. — Текст: непосредственный // Молодой ученый. — 2021.

Бизнинг шу бугунги холатимизда ахборот маконининг компютер тизимларидан анча узоқлашиб кетганлиги тўғрисидаги фикрларга қўшилмасликнинг иложи йўқ, Шу муносабат билан, «кибержиноят» атамаси “компютер жинояти” га қараганда кенгроқ маънога эга деган назарияни энг тўғри деб ҳисоблаш мақсадга мувофиқ бўларди.

Ушбу ёндашув вакиллари томонидан берилган таъриф кенгроқ ҳаракатлар доирасини ўз ичига олади ва замонавийлик талабларига яхшироқ
жавоб беради. Кибержиноятнинг моҳиятини яхшироқ тушуниш учун терминологиядан ташқари, ушбу турдаги жиноятларнинг ўзига хос белгиларини ҳам мукаммал ўрганиш керак бўлади. Бу умумий содир этилган жиноятлардан ахборот маконидаги жиноятларни алоҳида тахлилини олиб боришлик учун имконият беради хамда кибержиноятларга қарши курашнинг энг самарали чораларини белгилаб беради. Кўпгина тадқиқотчилар кибержиноятнинг ўзига хос хусусиятларини аниқладилар, ана шундай тадқиқотчилардан бири рус олим И.Г.Чекунов ички ва халқаро ҳуқуқий ҳужжатларни таҳлил қилиш асосида кибержиноятчилигининг нафақат жиноий
қилмишларининг ўзига хос белгиларининг тавсифи балки жиноятнинг субъектлари, мақсадлари ва жиноятни фош этишдаги мураккабликларини кўрсатиб бераолди.

Тадқиқот муаллифи И.Г.Чекунов кибержиноятчиликнинг қуйидаги фарқловчи белгиларини ажратиб кўрсатади:

-жиноятчилар ахборот-коммуникация технологияларидан фойдаланиш орқали ўз мақсадларига эришилади;

-кибержиноят трансчегаравий хусусиятга эга ва виртуал усулларда содир этилади;

-кибержиноятлар яширин тарзда содир этилади ва “ҳам давомли ҳамда бир марталик” жиноий холатлари бўлиши мумкин;

-бундай жиноятларга оид далилларни тўплаш қийин;

-ахборот маконида жиноятлар сонининг ўсиши бевосита технологик тараққиётнинг ривожланиши ва унинг натижаларига боғлиқ;

-кибержиноятларни субъекти асосан «ИТ технологиялари соҳасида чуқур билимга эга мутахассислари» хисобланади;

-кибержиноятлар асосан жудда катта миқёсда иқтисодий фойда олиш мақсадида содир этилади;

-кибержиноятларнинг гурухлар таркибида содир этилишига нисбатан ортиб бораётган тенденциялари мавжуд;

-жиноятларни фақат “ҳодисадан кейинги режимда” аниқлаш мумкин[35].

МУҲОКАМА ВА НАТИЖАЛАР

Юқоридаги кибержиноятларнинг ўзига хос хусусиятларидан келиб чиқиб, шуни хулоса қилиш мумкинки, кибержиноят бу кенг кўламли, юқори ўсиш суръатларига эга бўлган, субъектлари юқори интеллектуал маълумотлар билан ажралиб турадиган, асосан иқтисодий мақсадларга эга бўлган ва ундан

[35] Методические рекомендаций по расследованию приступлений в сфере компьютерной информации. Учебное пособие. Москва- 2018.

фойдаланадиган мураккаб жиноий харакат бўлиб, ушбу турдаги жиноятларни содир этишда жиноятчилар томонидан техника оламида энг янги тараққий этган техник воситаларидан фойдаланилади.

Ўзбекистон амалиётида Жиноят кодексининг XXI – бобида кўрсатилган фақат 6 турдаги жиноятлар кибержиноятлар сифатида тоифаланади ва ҲМҚО томонидан ушбу соҳадаги жиноятларнинг алоҳида ҳисоботи юритилмасдан келинмоқда. МДҲ аъзо давлатларда кибержиноятчилик тушунчаси юзасидан

турлича қарашлар шаклланган бўлиб, ягона ёндашув мавжуд эмас.

Европа мамлакатларида кибержиноятларга - АТ ёрдамида, хусусан, Интернет глобал тармоғидан фойдаланиб содир этилаётган барча жиноятлар киритилиб, уларнинг статистикаси ҳам алоҳида юритилиб борилади, мазкур ҳолат ушбу турдаги жиноятларни мониторинги ҳамда унга қарши курашишда куч ва воситаларни бошқаришда қулайлик яратади.

Кибержиноятлар – қарийб 90 фоизи латентлиги, айбдорнинг шахсини, ҳодиса жойини аниқлаш мураккаблиги, ҳудуд жиҳатидан аксарияти бошқа давлатда содир этилиши (трансчегаравийлиги) ҳамда далилларни тўплаш қийинлиги хусусиятларига кўра айбдор шахслар аниқланмасдан қолиш ҳолатлари кузатилмоқда.

Сўнгги пайтда катта аудиторияга эга бўлган Facebook, Microsoft, Twitter ва YouTube хусусий компаниялари кибертерроризмга қарши курашиш мақсадида бирлашиш, бу борада рахбарий тамойилларни яратиш, янги усул ва методларни ишлаб чиқишда ўзлари ташаббускорлик кўрсатишмоқда.

Жумладан, 2016 йилда мазкур нодавлат ташкилотлар БМТ Хавфсизлик кенгашининг Контртерроризм қўмитаси ва Европа Иттифоқи билан ҳамкорлик ўрнатиб, АТ соҳасидаги жиноятларни фош этиш юзасидан маълумот алмашиш, ўқув семинарларини ташкил этишга тайёр эканликларини маълум қилишди.

Мазкур соҳада халқаро ва минтақавий ташкилотлар амалиёти таҳлил қилинганида, АТ соҳасидаги жиноятларга қарши курашишда мазкур соҳадаги муносабатларни тўла қамраб оладиган, инсон ҳуқуқларини ҳимоя қилувчи умумжахон конвенция, шартномаларга мувофиқ миллий қонунчиликни такомиллаштириш, янги жиноий ҳолатлар юзасидан жиноий тақиқни ўрнатишни тавсия этилаётганлиги кузатилмоқда.

Хусусан, БМТ Бош Ассамблеянинг 65/230 сонли кибержиноятчилик юзасидаги “Ҳукуматлараро мутахассислар маслаҳатлашув гуруҳи” резолюцияси ва 2001 йилда қабул қилинган “Будапешт” Европа конвенцияси ҳамда Бутунжахон стандартлаштириш ташкилоти (БСТ) томонидан 2015 йилда ўрнатилган Ўзбекистон Республикаси Президенти Шавкат Мирзиёев шахсан ҳуқуқбузарликлар профилактикаси соҳасини такомиллаштириш, уларнинг содир этилиши сабаблари ва имкон берган шарт-шароитларни бартараф этиш юзасидан фикр ва мулоҳазаларини билдириб бу масалалар нақадар муҳим эканлигини кўрсатиб берди.

“Ҳудудлардаги криминоген вазиятни чукур таҳлил қилиш, жиноятларнинг динамикаси ва содир этилишига таъсир қилаётган омилларни аниқлаш ва “илмий

диагноз” қўйиш орқали жиноятчиликни прогнозлаш ва унинг олдини олишга алоҳида эътибор қаратилмоқда”[36], - деб таъкидлаб ўтган.

Хусусан, Самарқанд вилоятининг кибержиноятларнинг холати ўрганиб 2021 йилнинг 9 ойи давомида чиқилганида, ушбу турдаги жиноятларнинг аксарияти пластик карталар орқали фирибгарлик билан боғлиқ ҳолатда содир этилганлиги, фуқароларнинг сир сақлаши лозим бўлган шахсий маълумотларини ошкор қилишлари сабаб бўлмоқда.

Масалан: 2020 йил 19 декабрь куни Жомбой тумани янги хаёт МФЙда яшовчи 21.02.2001 йилда туғилган фуқаро “П” Самарқанд вилояти ИИБ бошлиғи номига ариза билан мурожаат қилиб, унда 2020 йил 14 октябрь куни соат 16:13лар атрофида Самарқанд шаҳар А.Қушчи кўчаси “Скрининг маркази” олдида турмуш ўртоғига тегишли бўлган Самасунг S6 маркали телефон аппаратидан телеграм мессенжерига кириб, “Микроқарз Админ” номли аккаунтдан микроқарз расмийлаштириб бериш тўғрисида келган хабарга жавобан микроқарз расмийлаштириб олмоқчи бўлиб, турмуш ўртоғи М.Темурхоновга тегишли паспорт ҳамда Миллий банк пластик картасини телеграм орқали жўнатиб, телефонига “OSON” иловаси орқали келган махфий кодни ушбу профил фойдаланувчисига юборгандан сўнг пластик картадаги жами 4.622.000 сўм пуллари номаълум шахс томонидан ечилганлигини маълум қилган. Самарқанд вилояти ички ишлар бошқармаси ходимлари томонидан олиб борилган тезкор техник тадбирлар натижасида Қашқадарё вилояти Чироқчи тумани Дам ҚФЙда яшовчи, бўйдоқ, муқаддам судланмаган, вақтинча ишсиз, 2020 йилда Ал-Хоразмий номидаги Тошкент ахборот техналогиялари университетини тугатган, 24.05.1995 йилда туғилган “Б” исмли фуқоро Тошкент шаҳри Чилонзор тумани ҳудудидан ушланиб, ундан 3 дона қўл телефон аппарати, Алоқа банк номига расмийлаштирилган пластик картаси далилий ашё сифатида хужжатлаштирилиб олинган.

Фуқоро “Б” билан олиб борилган суриштирув ишлари давомида у ушбу фаолият билан 2020 йил тахминан март ойларидан буён шуғулланиб келишини, жабрланувчиларни асосан “Mikroqarz Admin”, “Dilmurod Mikroqarz”, “Bankir Mikroqarz” номли “2ndLine” дастуридан фойдаланиб турли давлатлар рақамларига очилган телеграм профилларидан кириб банкда ишлашини ҳамда қисқа вақтда микроқарз расмийлаштириб беришини айтиб, фуқароларни алдаб уларга тегишли пластик карталарига “OSON”, “PAYME”, “Click”, “Apelsin” иловаларидан фойдаланиб жабрланувчиларни карталарига уланиб олиб, ушбу пулларни асосан “Qiwi” электрон хамёни орқали айлантириб ўзига тегишли +998900020064 рақамига очилган Id 212604027 бўлган “1хбет” букмекрлик фаолиятига асосланган ўйинларга тикиш билан йўтқазиб, қолган пулларни ўз эхтижига сарфлаганлигини маълум қилган.

Фуқоро “Б”нинг Редми Нот 8 русумли телефон аппарати холислар иштирокида кўздан кечирилганда Ўзбекистон Республикасининг турли вилоятларида яшовчи 143 нафар фуқароларнинг паспорт маълумотлари, телеграм аккаунтидаги “Mikroqarz Admin” номи остида очилган профили, “Qiwi”

[36] https://ejarima.uz/uz/news/sotrudnikam-i-veteranam-organov-vnutrennih-del

ва “1хбет” электрон хамёнларида тахминан 50 млн сўмдан ортиқ пулларни айлантирганлиги аниқланган, ҳозирда ушбу холат юзасидан қонун билан белгиланган тартибда тергов харакатлари олиб борилмоқда.

ХУЛОСА Шуни таъкидлаш лозимки, жабрланувчиларнинг ўзлари пластик карталарининг рақамларини жиноятчиларининг алдовига кириб ошкор қилишган, бу уларнинг ишонувчанлиги ва тезроқ бойлик орттиришга бўлган қизиқишлари сабабли содир бўлган.

Шу боисдан, ушбу соҳадаги жиноятларнинг олдини олишда биринчидан, фуқаролар ўртасида пластик карталари рақамларини ошкор қилмасликлари, иккинчидан, шартномаларни фақатгина нотариал тартибда амалга оширишлари, учинчидан, телефон орқали алоқага чиққан ҳар қандай шахсларнинг сўзларига ишонмасликлари ва бу ҳақда зудлик билан ИИОларига хабар беришлари лозимлиги ҳақидаги виктимологик чора-тадбирларни амалга ошириш лозимдир.

Бунда жиноят содир этилишига олиб келган детерминатларни ҳам ўрганиш мақсадга мувофиқдир. Криминология фанида криминоген вазиятга таъсир этувчи омилларни детерминантлар дейилади. Жиноятчиликнинг моҳияти ва қонуниятлари унинг миқдор ва сифат кўрсаткичларини ўрганиш орқали очиб берилади. “Детерминация”, яъни воқеа, ҳодиса ва жараёнлар ўртасидаги боғлиқликни билдирувчи алоқа ҳақидаги назариядан фойдаланилади. Диалектик детерминизм табиат ва жамиятдаги барча ҳодисалар, жумладан кишиларнинг ирода ва хулқларининг умумий объектив қонунияти борлиги ва улар бир-бирига боғлиқ бўлиб, бир-бирини тақозо этишини эътироф этувчи назариядир[37].

Шу мақсадларни инобатга олган ҳолда қуйидаги ташкилий вазифаларни:

биринчидан, тергов амалиётида мунтазам равишда кибер жиноятчилик таҳлилини юритиш;

иккинчидан, ахборот-коммуникация жабҳасидаги жиноятларнинг мунтазам профилактикасини йўлга қўйиш;

учинчидан, компьютер ҳамда ахборотлаштириш соҳасидаги жиноятларга нисбатан «Кибер таҳдидга қарши Кибер мудофаа» корпусини ташкил қилиш;

тўртинчидан, соҳада малакали кадрларга бўлган эҳтиёждан келиб чиқиб, зудлик билан етук мутахассис ходимлар тармоғини яратиш;

бешинчидан, энг аввало мулкчилик шаклидан қатъи назар, барча корхона, ташкилот, муассасалардаги компьютер ва дастурий таъминот қурилмалари учун кучли пароллар ва шифрлар тизимини йўлга қўйиш;

олтинчидан, мавжуд пароллар тизимини ҳар 3 ойда янгилаб туриш механизмларини жорий этиш;

еттинчидан, ахборотлаштириш ҳамда дастурлаш соҳаси юзасидан четдан мутахассис жалб этиш анъаналаридан босқичма-босқич воз кечиб, тергов идоралари тизимида мустақил экспертлар тизимини шакллантириш билан боғлиқ тадбирларни мавжуд имкониятлардан келиб чиқиб амалга ошириш зарурдир.

[37] Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24.

Юқорида қайд этилган таклифларни ўз вақтида амалиётга татбиқ этилиши, келгусида ИТ-соҳасида қонунларга ҳурмат руҳи шаклланишига ва мазкур муносабатлар тизимида ҳуқуқий интизомни ташкил топишига замин яратади.

Адабиётлар рўйхати.

1. Шарыпова Т. Н., Сидоренко А. А. Киберпреступность в XXI веке // Аллея науки. № 1. 2019 года.
2. Чекунов И.Г. Киберпреступность: понятие,классификация, современные вызовы и угрозы // Журнал Молодые ученые № 3. 2012 года.
3. Глобальная угроза экономической безопасности: виды, особенности, проблемы воздействия // Ростовский научный журнал № 1. 2018 года.
4. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 года.

KIBERXAVFSIZLIKNING OLDINI OLISHDA ICHKI ISHLAR ORGANLARINING O‘RNI

Axmedov Farxod Saydalievich

Malaka oshirish instituti Kasbiy tayyorgarlik fakulteti Maxsus fanlar sikli o‘qituvchisi
+99899 8226327

Annotatsiya: *Mazkur maqolada kiberxavfsizlikning oldini olishda ichki ishlar organlari apparat, apparat-dasturiy va dasturiy vositalardan foydalangan holda qasddan amalga oshiriladigan, kiberxavfsizlikka tahdid soladigan, shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui, yoshlarning ongini, zo‘ravonlikka, milliy o‘zligini, madaniy-ma’rifiy va oilaviy qadriyatlarini yo‘qotishga undash yo‘li bilan jamiyatda zo‘ravonlik va radikal qarashlarni tarqatishning oldini olish hamda asosiy tushunchalar ko‘rsatilgan.*

Tayanch so‘zlar: *kiberjinoyatchilik, kibermakon, kibertahdid, kiberxavfsizlik, kiberhimoya, kiberhujum, Youtube, Telegram, Instagram.*

Aholining tinch va osoyishta hayotini ta’minlash, jinoyatchilik va huquqbuzarliklarga qarshi kurashish, jamoat tartibini saqlash – bugungi kunda eng muhim vazifadir.

Shavkat Mirziyoev

Bugun mamlakatimizda barcha jabhada amalga oshirilayotgan islohotlar yanada jadal tus olmoqda. Ko‘zlangan marralar esa aniq. Bu taraqqiyot sari ilgarilama harakat. Bu yangilanish va zamonaviylashish. Bu nafaqat iqtisodiyot va ishlab chiqarishni modernizatsiya qilish. Bu yangicha fikrlash, yangicha dunyoqarash, hayotga, ishga, o‘qishga bo‘lgan munosabatni o‘zgartirishdir.

Prezidentimiz Shavkat Mirziyoev: **«Xalqimiz yaratgandan avvalo tinchlik-xotirjamlikni so‘raydi. Shundan so‘ng o‘z uyim, boshpanam bo‘lsa, oilam, bola-chaqam bilan sog‘-salomat yashasam, deydi. Biz xalqimizning ana shunday orzu-niyatlarini ro‘yobga chiqarish uchun ikkita masalaga, ya’ni ichki ishlar va sog‘liqni saqlash tizimini isloh qilishga alohida e’tibor qaratayapmiz»** deganlarida tinchlik-xotirjamlikning inson, jamiyat, davlatning eng muhim hayotiy manfaatlarini ro‘yobga chiqarishdagi o‘rni hamda bu buyuk ne’matni ta’minlash umummilliy vazifa ekanligini nazarda tutadi.

Jumladan, Kiberxavfsizlik XX-asrning ikkinchi yarmi va XXI-asrda jahon mamlakatlari, xalqlari hayotiga tahdid soluvchi, jamiyatda beqarorlik va qo‘rquv uyg‘otish, axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan unumli foydalanishlar avj olib ketdi.

Bugungi dolzarb zamonda raqamli texnologiyalar barcha sohalarga va odamlar hayotiga jadal kirib bormoqda. Ushbu soha rivojlanib borgani sari, bundan g‘araz maqsadda foydalanuvchilar ham ortmoqda. Hozirgi kunda, viloyat hududida sodir etilayotgan jami jinoyatlar orasida internet va kompyuter texnologiyalari bilan bog‘liq jinoyatlar keskin oshmoqda.

Joriy yilning 9 oyi mobaynida ushbu turdagi murojaatlar soni 2 barobarga oshgan. Natijada fuqarolarga 4 milliard so‘mga yaqin zarar yetkazilgan.

Ushbu holatlarning oldini olish va aholining ogohligini oshirish maqsadida Prezidentimizning 2022-yil 3-fevraldagi “Internet tarmog‘ida sodir etilayotgan huquqbuzarliklarning barvaqt oldini olishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi qarori qabul qilindi. Qarorga muvofiq, Respublika hududida bu turdagi huquqbuzarliklarning oldini olish bo‘yicha kompleks targ‘ibot-tashviqot tadbirlari Ichki ishlar organlarining tashabbusi bilan o‘tkazilishi belgilangan.

Agar O‘zbekiston Respublikasining xalqaro shartnomasida O‘zbekiston Respublikasining kiberxavfsizlik to‘g‘risidagi qonunchiligida nazarda tutilganidan boshqacha qoidalar belgilangan bo‘lsa, xalqaro shartnoma qoidalarida qo‘llanilishi ko‘rsatib o‘tilgan.

Kiberxavfsizlik to‘g‘risidagi qonunda quyidagi asosiy tushunchalar qo‘llaniladi:

axborotlashtirish ob’ekti — turli darajadagi va maqsaddagi axborot tizimlari, telekommunikatsiya tarmoqlari, axborotga ishlov berishning texnik vositalari, ushbu vositalar o‘rnatilgan va foydalaniladigan xonalar;

kiberjinoyatchilik — axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi;

kibermakon — axborot texnologiyalari yordamida yaratilgan virtual muhit;

kibertahdid — kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui;

kiberxavfsizlik — kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati;

kiberxavfsizlik hodisasi — kibermakonda axborot tizimlarining ishlashida uzilishlarga va (yoki) ulardagi axborotning ochiqligi, yaxlitligi va undan erkin foydalanilishining buzilishiga olib kelgan hodisa;

kiberxavfsizlik ob'ekti — axborotning kiberhimoya qilinishini hamda milliy axborot tizimlari va resurslarining kiberxavfsizligini ta'minlashga doir faoliyatda foydalaniladigan axborot tizimlari majmui, shu jumladan muhim axborot infratuzilmasi ob'ektlari;

kiberxavfsizlik sub'ekti — milliy axborot resurslariga ega bo‘lish, ulardan foydalanish va ularni tasarruf etish hamda ulardan foydalanish bo‘yicha elektron axborot xizmatlari ko‘rsatish, axborotni himoya qilish hamda kiberxavfsizlik bilan bog‘liq muayyan huquqlar va majburiyatlarga ega bo‘lgan yuridik shaxs va (yoki) yakka tartibdagi tadbirkor, shu jumladan muhim axborot infratuzilmasi sub'ektlari;

kiberhimoya — kiberxavfsizlik hodisalarining oldini olishga, kiberhujumlarni aniqlashga va ulardan himoya qilishga, kiberhujumlarning oqibatlarini bartaraf etishga, telekommunikatsiya tarmoqlari, axborot tizimlari hamda resurslari faoliyatining barqarorligini va ishonchliligini tiklashga qaratilgan huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik chora-tadbirlar, shuningdek ma'lumotlarni kriptografik va texnik jihatdan himoya qilish chora-tadbirlari majmui;

kiberhujum — kibermakonda apparat, apparat-dasturiy va dasturiy vositalardan foydalangan holda qasddan amalga oshiriladigan, kiberxavfsizlikka tahdid soladigan harakat;

muhim axborot infratuzilmasi — muhim strategik va ijtimoiy-iqtisodiy ahamiyatga ega bo‘lgan avtomatlashtirilgan boshqaruv tizimlarining, axborot tizimlari hamda tarmoqlar va texnologik jarayonlar resurslarining majmui;

muhim axborot infratuzilmasi ob'ektlari — davlat boshqaruvi va davlat xizmatlari ko‘rsatish, mudofaa, davlat xavfsizligini, huquq-tartibotni ta'minlash, yoqilg‘i-energetika majmui (atom energetikasi), kimyo, neft-kimyo tarmoqlari, metallurgiya, suvdan foydalanish va suv ta'minoti, qishloq xo‘jaligi, sog‘liqni saqlash, uy-joy kommunal xizmatlar ko‘rsatish, bank-moliya tizimi, transport, axborot-kommunikatsiya texnologiyalari, ekologiya va atrof-muhitni muhofaza qilish, strategik ahamiyatiga ega bo‘lgan foydali qazilmalarni qazib olish va qayta ishlash sohasida, ishlab chiqarish sohasida, shuningdek iqtisodiyotning boshqa tarmoqlarida va ijtimoiy sohada qo‘llaniladigan axborotlashtirish tizimlari;

muhim axborot infratuzilmasi sub'ektlari — davlat organlari va tashkilotlari, shuningdek mulk, ijara huquqlari asosida yoki boshqa qonuniy asoslarda muhim axborot infratuzilmasi ob'ektlariga egalik qiluvchi yuridik shaxslar, shu jumladan muhim axborot infratuzilmasi ob'ektlarining ishlashini hamda hamkorligini ta'minlovchi yuridik shaxslar va (yoki) yakka tartibdagi tadbirkorlar[38].

Kiberxavfsizlikni ta'minlashning asosiy prinsiplari quyidagilardan iborat:

- qonuniylik;
- kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning

[38] *Manba. O‘zbekiston Respublikasining 2022-yil 15-aprel kunidagi "Kiberxavfsizlik to‘g‘risida"gi O‘RQ-764-son Qonuni.*

ustuvorligi;

- kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv;
- kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;

***Kiberxavfsizlik bu*- u** kompyuterlar, serverlar, mobil qurilmalar, tarmoqlar va elektron tizimlar orqali yaratilgan va qayta ishlanadigan ma'lumotlarni himoya qilish uchun amalga oshiriladigan protseduralar va vositalar to‘plami sifatida belgilanishi mumkin.

Oddiy qilib aytganda, kiberxavfsizlik – bu muhim tizimlar va nozik ma'lumotlarni raqamli hujumlardan himoya qilish amaliyotidir.Yaqin yillarda kiber jinoyatchilikning eng yirik turi - yuqori malakali kiber jinoiy guruhlar ko‘payishi va ifratuzilmaga hujum uyushtirilishidan iborat bo‘ladi, deydi “Laboratorii Kasperskogo” rahbari Yevgeniy Kasperskiy “RIA Novosti” muxbiri bilan suhbatda.Birinchi trend – kiber jinoyatchilik ommaviy tus oladi. Taassufki, iqtisodiy inqiroz davrida ushbu illat ayniqsa ko‘p urchiydi. Jinoyatchilar safi endi-endi to‘lib kelmoqda, - deydi u.

Olimning ta'kidlashicha, “Kaspersky Security Network” ma'lumotiga ko‘ra, iyul oyida dunyo bo‘yicha har kuni 400 mingdan ortiq zarar keltiruvchi dasturiy ta'minot paydo bo‘lgan. “Har kuni shuncha zararli virus tarqatish uchun qancha xaker zarur bo‘ladi, bu savolga javob berish mushkul”, deydi u. “Albatta, ularda avtomatlashtirish, kodlarni avtomatik generatsiyalash imkoni mavjud. Umuman, xakerlar soni 100 mingdan ortiq, deyishsa, hayron qolmagan bo‘lardi, - qo‘shimcha qildi Kasperskiy.

Ikkinchi trend – yuqori malakali kiber jinoyatchi guruhlar paydo bo‘lishi. Darvoqe, ilk shunday tuzilma – “Sarbanak” guruhi 2014-yilda paydo bo‘lgan edi. Bungacha davlatlar homiylik qilgan xakerlar va oddiy jinoyatchilar faoliyat olib borishgan. “Sarbanak” ortidan yana ko‘plab professional guruhlar paydo bo‘ldi, – deydi mashhur dasturchi.

Uchinchi trend – infratuzilmaga hujum uyushtiruvchilar safi keyingi yillarda borgan sari kengaymoqda. “Sur'atiga baho bera olmayman, chunki ular qaysi yo‘ldan yuradi, bunday guruhlar uchun qaysi mavzu dolzarb ekanini oldindan aytish qiyin. Jinoyatchilar faoliyati ko‘p omillarga bog‘liq. Hujumlar murakkablashadi, borgan sari ko‘p texnologiyalar hujum ostida qoladi, lekin hujum qaysilariga uyushtirilishi va qanday tartibda kechishi siz bilan bizga bog‘liq emas, - qo‘shimcha qildi u.

Kasperskiy dunyoning turli hududlaridagi xakerlarning ixtisoslashuvi haqida ham so‘z yuritib, xitoylik kiber jinoyatchilar ko‘proq botnetlar (zararli dasturiy ta'minot bilan zararlantirilgan kompyuterlar tarmog‘i), rossiyaliklar dasturlash – raqamli belgilarni aniqlash, Lotin Amerikasi xakerlari esa moliyaviy qallobliklar bo‘yicha ish olib boradi.

Eng qizig‘i, jinoyatchilarda ixtisoslashuv mavjud. Xitoyliklar ko‘proq botnetlar bilan ishlaydi, raqamli kodlardan foydalanuvchi xakerlar tez-tez ruscha so‘zlashadi, moliyaviy tovlamachilik bilan shug‘ullanuvchi xakerlar asosan Lotin Amerikasi mintaqasidan, - deydi u[39].

O‘zbekiston Respublikasi Prezidenti Sh.M.Mirziyoev 2023-yil davomida ichki ishlar organlari faoliyati samaradorligini oshirish, fuqarolarning huquq va

[39] *Manba. O‘zbekiston Milliy axborot agenligi.*

erkinliklarini ta’minlash maqsadida bir qator quyidagi kompleks chora-tadbirlar amalga oshirilishiga qaramasdan quyidagi jinoyatlar sodir etilgan.

Kiberxavfsizlik yo‘nalishida 6 455 ta jinoyatlar sodir etilgan bo‘lib, ularning 76 foizi ya’ni (4 923 ta) fuqarolarning bank plastik kartalaridagi pullarni qo‘lga kiritish bilan bog‘liqdir. Elektron to‘lov tizimlari orqali sodir etilgan jinoyatlarning 53 foizi (2619 tasi) soxta havolalar yuborish orqali tasdiqlovchi kodni qo‘lga kiritib, karta boshqaruvini egallash yo‘li bilan, 15 foizi (734 tasi) onlayn savdo platformalarida turli aldovlar bilan tovarlar uchun to‘lovni oldindan amalga oshirishga erishish orqali, 13,2 foizi (651 tasi) telefon qo‘ng‘iroqlari orqali bank karta boshqaruvini tasdiqlovchi kodni qo‘lga kiritish yo‘li bilan sodir etilgan. Shuningdek, 11,8 foizi (577 tasi) shaxslarni soxta kripto-birjalarga qiziqtirish va pul o‘tkazishga erishish orqali, 1,4 foizi (68 tasi) xorijdan pul yuborishni va’da qilib, pochta xarajatlariga to‘lov sifatida pul o‘tkazdirish orqali sodir etilgan. Internet tarmog‘ida noqonuniy ravishda onlayn qimor va tavakkalchilikka asoslangan o‘yinlarni o‘tkazib, fuqarolarning pul mablag‘larini jalb etib kelayotgan 420 ta internet resurslari aniqlanib, bloklandi hamda ularni sodir etgan 95 nafar shaxslar ma’muriy va jinoiy javobgarlikka tortildi. Kibertovlamachilik qilib kelgan 421 ta internet resurslarning faoliyati aniqlanib, barchasi bloklandi hamda 15 nafar shaxs jinoiy javobgarlikka tortildi, 54 nafar shaxs rasmiy ogohlantirildi. Aholini kibertahdidlardan ogohlantirish bo‘yicha “Cyber-Week” va “Cyber 10 day” nomlari ostida jami 46 047 ta kompleks targ‘ibot-tashviqot tadbirlari o‘tkazilib, 17 mln 903 ming aholi qamrab olindi. Mahallalarda 15 102 ta, maktablarda 12 134 ta, oliy ta’lim muassasalarida 1 593 ta, korxonalarda 7 201 ta hamda savdo komplekslarida 2701 ta targ‘ibot tadbirlari o‘tkazilgan. Qamrab olingan aholining 7 mln 206 ming nafari hududlarda olib borilgan targ‘ibot-tashviqot tadbirlari davomida, 10 mln 697 ming nafari esa ijtimoiy tarmoqlardagi targ‘ibot kanallari orqali tegishli ma’lumotlar bilan tanishdi. Kiberjinoyatlardan himoyalanish usullarini tushuntiruvchi 35 087 ta videokontent, 429 216 ta tarqatma material va 12 909 ta bannerlar tayyorlandi, ommaviy axborot vositalarida 13 633 marotaba chiqishlar qilindi. Ichki ishlar vazirligining (“Youtube”, “Telegram”, “Instagram”) ijtimoiy tarmoqlardagi “cyber 102 |IIV Kiberxavfsizlik markazi” targ‘ibot kanallari orqali 400 mingdan ortiq obunachiga 39 176 ta tashviqot materiallari havola etildi.

Mamlakatimizning har bir fuqarosi ichki ishlar organlari xodimi timsolida o‘zining xayoti, sog‘ligi, sha’ni va qadr-qimmatini har qanday tajovuzlardan muhofaza qilishga va og‘ir damda yordam berishga tayyor bo‘lgan himoyachisini ko‘rishi hamda o‘zining havfsizligi ta’minlanganligini his qilishi zarur.

Prezidentimiz ichki ishlar organlarining kasb bayrami munosabati bilan yo‘llagan tabrigida ***«Agar davlat tayanadigan asosiy ustun qonun bo‘lsa, uning kuchini amalda namoyon etadigan eng samarali tizim bu – ichki ishlar sohasi, desak, ayni haqiqat bo‘ladi»,*** deya e’tirof etgan edi. Bu yuksak baho osoyishtalik posbonlarini qonun ustuvorligini ta’minlash yo‘lida yanada fidoyilik bilan xizmat qilishga undaydi.

Xulosa o‘rnida ichki ishlar organlari xodimlari jinoyatchilik va huquqbuzarlik uchun omil bo‘layotgan kiberxavfsizlik odatda kibertahdidlar va kiberjinoyatlar va shu kabi boshqa illatlarning vaqtida oldini olish choralaridan tashqari, kibermakonda

shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holatini aniqlashda ichki ishlar organlari muhim o‘rin tutadi.

FOYDALANILGAN ASOSIY ADABIYOTLAR

1. O‘zbekiston Respublikasining Konstitutsiyasi. –T., 2023-yil
2. O‘zbekiston Respublikasining 2016-yil 16-sentyabrdagi “Ichki ishlar organlari to‘g‘risida”gi O‘RQ-407-son Qonuni;
3. O‘zbekiston Respublikasining 2022-yil 15-aprel kunidagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni.
4. O‘zbekiston Respublikasi Prezidentining 2022-yil 3-fevraldagi “Internet tarmog‘ida sodir etilayotgan huquqbuzarliklarning barvaqt oldini olishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarori

KIBERJINOYATLARGA QARSHI XALQARO KELISHUVLAR VA ULARNING MILLIY QONUNCHILIKKA IMPLEMENTATSIYASI

Komilov Lazizjon Zokirjon o‘g‘li

IIV Malaka oshirish instituti Jangovar tayyorgarlik sikli o‘qituvchisi

Obro‘ga ega bo‘lish uchun yigirma yil kerak, uni yo‘qotish uchun esa bir necha daqiqalik kiberhujum kifoya

Stefan Nappo

Bugungi kunda global axborot maydonida kibermakon bilan bog‘liq yangidan-yangi tahdidlar yuzaga kelmoqda. Shu bois virtual olamdagi hujumlardan himoyalanish masalasi dunyo hamjamiyatini jiddiy tashvishga solmoqda. Raqamli iqtisodiyotning rivojlanishi va axborot texnologiyalarining keng ommalashuvi natijasida kiberjinoyatchilik zamonaviy jamiyat uchun jiddiy tahdidlardan biriga aylandi. Ushbu global muammo faqat milliy darajada emas, balki xalqaro hamkorlik asosida samarali hal qilinadi. Shu sababli, xalqaro kelishuvlar va konvensiyalar kiberjinoyatlarga qarshi kurashda muhim huquqiy asoslarga ega. Shu munosabat bilan O‘zbekiston Respublikasida mutasaddi tashkilotlar tomonidan kiberjinoyatchilikka qarshi kurashishda samaradorlikka erishishi uchun xalqaro kelishuvlarga qo‘shilishi, ularning milliy qonunchilikka moslashtirilishi va amaliyotga tatbiq etilishi jarayonlari tashkil etilishi lozim.

O‘zbekiston Respublikasida kiberxavfsizlik sohasidagi munosabatlar va kiberjinoyatlarga qarshi kurashish O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni hamda boshqa qonunosti hujjatlari orqali tartibga solinadi. Mazkur qonunda “**kiberjinoyatchilikka –** axborotni egallash, uni o‘zlashtirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi[40]” deya ta’rif berilgan.

[40] O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni 3-moddasi;

Tahlillarga ko‘ra, dunyo bo‘ylab har yili 500 milliondan ortiq kiberhujumlar uyushtiriladi. Har soniyada 12 nafar insondan biri kiber makonda sodir etilgan hujumlar qurboniga aylanadi. Amerika Qo‘shma Shtatlari, Fransiya, Angliya, Germaniya, Belgiya, Lyuksemburg kabi rivojlangan davlatlarda jinoyatlarning 60-65 foizi kiber hujumlar orqali sodir etilmoqda. O‘zbekistonda ham so‘nggi uch yilda bu turdagi jinoyatlar 8,3 baravarga ko‘payib, hozirda umumiy jinoyatchilikning qariyb 5 foiziga yetgan. Xususan, noqonuniy bank-moliya operatsiyalari orqali o‘zgalarning plastik kartadagi mablag‘larini o‘zlashtirish, zararli viruslar tarqatish, qimor va tavakkalchilikka asoslangan onlayn o‘yinlar, diniy aqidaparastlikka qaratilgan axborot xurujlari, onlayn savdo maydonidagi firibgarlik jinoyatlari ko‘payib bormoqda

Achinarlisi, axborot texnologiyalari yordamida huquqbuzarlik va jinoyatga qo‘l urgan shaxslar orasida yoshlar ko‘pchilikni tashkil etmoqda. Respublikamizda virtual olamdagi qonunbuzilishlarning aksariyati 16-23 yosh oralig‘idagi o‘smir-yoshlar tomonidan sodir qilinmoqda. Bundan ko‘rinib turibdiki, kiberxavfsizlikni ta’minlash masalasi bugun har qachongidan ham dolzarb ahamiyat kasb etmoqda[41].

Kiberjinoyatlarni butunlay yo‘q qilish va to‘liq internet xavfsizligini ta’minlash imkoni bo‘lmasa-da, korxonalar, tizimlar, tarmoqlar va ma’lumotlar xavfsizligini ta’minlashga chuqur mudofaa yondashuvidan foydalangan holda samarali kiberxavfsizlik strategiyasini qo‘llab-quvvatlash orqali uning ta’sirini kamaytirishga erishish mumkin. Kiberjinoyat xavfini quyidagi qadamlar bilan kamaytirish mumkin: biznes va xodimlar uchun aniq siyosat va tartiblarni ishlab chiqish; ushbu siyosat va protseduralarni qo‘llab-quvvatlash uchun kiberxavfsizlik hodisalariga javob rejalarini yaratish; tizimlar va korporativ ma’lumotlarni himoya qilish bo‘yicha amaldagi xavfsizlik choralarini belgilash; ikki faktorli autentifikatsiya (2FA) ilovalari yoki jismoniy xavfsizlik kalitlaridan foydalanish; imkoni bo‘lganda har bir onlayn hisobda 2FAni faollashtirish; moliyaviy menedjer bilan gaplashish orqali pul jo‘natish bo‘yicha so‘rovlarning haqiqiyligini og‘zaki tekshirish; kompaniya electron pochta xabarlariga o‘xshash kengaytmali electron pochta xabarlarini belgilovchi tajovuzlarni aniqlash tizimi (IDS) qoidalarini yaratish; so‘rovlar odatiy emasligini aniqlash uchun pul mablag‘larini o‘tkazish bo‘yicha barcha elektron pchta so‘rovlarini diqqat bilan ko‘rib chiqish; xodimlarni kiberxavfsizlik siyosati va tartbi-qoidalari hamda xavfsizlik buzilgan taqdirda nima qilish kerakligi bo‘yicha doimiy ravishda o‘qitish; veb-saytlar, so‘nggi nuqta qurilmalari va tizimlarini barcha dasturiy ta’minot yangilanishlari yoki tarmoqlari bilan joriy etish; ransomware hujumi yoki ma’lumotlar buzilgan taqdirda zararni kamaytirish uchun ma’lumotlar va ma’lumotlarni muntazam ravishda zaxiralash[42].

Yevropada Kiberjinoyatchilikka qarshi kurashishda Budapesht konvensiyasining huquqiy o‘rni beqiyosdir. Budapest konvensiyasi (rasmiy nomi - Kiberjinoyatchilikka qarshi konvensiya) 2001-yilda Yevropa Kengashi tomonidan ishlab chiqilgan bo‘lib, kiberjinoyatlarga qarshi kurashda xalqaro huquqiy me’yorlarning asosini tashkil etadi. Ushbu konvensiya:

[41] https://akadmvd.uz/oz/news/kiber-makonda-sodir-etilaetgan-zhinojatlarga-arshi-kurashish

[42] “Kiberjinoyatchilikka qarshi immunitet hosil qilish masalalari” B.O.Primov / Ilmiy maqola / 164-b.

- kompyuter tizimlariga noqonuniy kirish, ma'lumotlarni buzish yoki o‘g‘irlash, kompyuter firibgarligi va boshqa jinoyatlarni jinoyat sifatida belgilaydi;

- a’zo davlatlar o‘rtasida huquqiy yordam va ma’lumot almashinuvini nazarda tutadi;

- tezkor axborot almashinuvi va kiberhujumlarni tekshirish mexanizmlarini tartibga soladi.

Bundan tashqari, kiberjinoyatlarga qarshi kurash bo‘yicha BMT, MDH, va boshqa xalqaro tashkilotlar tomonidan bir qator tashabbuslar ishlab chiqilgan. Bunga BMTning 2021-yilda qabul qilingan "Raqamli erkinlik va xavfsizlik" rezolyutsiyasi misol bo‘la oladi.

Kiberjinoyatlar transmilliy xarakterga ega bo‘lgani uchun xalqaro hamkorlik ushbu jinoyatlar bilan samarali kurashishning ajralmas qismidir. Xalqaro kelishuvlar davlatlararo huquqiy hamkorlikni mustahkamlash, jinoyatchilarni izlash va sudga tortishda muhim o‘rin tutadi. O‘zbekiston Respublikasi 2023-yilda Budapesht konvensiyasiga qo‘shilish jarayonini boshlagan. Bu jarayon O‘zbekistonning xalqaro huquqiy standartlarga intilishi va kiberxavfsizlikni mustahkamlash borasidagi harakatlarini aks ettiradi.

MDH davlatlari o‘rtasida esa kiberjinoyatlarga qarshi kurashish bo‘yicha 2018-yilda qabul qilingan “Kiberxavfsizlik to‘g‘risidagi bitim”ga O‘zbekiston a’zo hisoblanadi. Ushbu bitim MDH davlatlari o‘rtasida ma’lumot almashish, qo‘shma tadbirlar o‘tkazish va jinoyatlarni tekshirishda huquqiy yordamni ta’minlaydi.
Shuningdek, 2020-yilda O‘zbekiston BMTning Kiberxavfsizlik bo‘yicha maxsus ishchi guruhiga qo‘shilib, xalqaro miqyosda o‘z tajribasini oshirishga kirishdi. Bundan tashqari, davlat AQSh, Janubiy Koreya, va Xitoy kabi mamlakatlar bilan ikki tomonlama kiberxavfsizlik bitimlarini ishlab chiqmoqda.

Hozirgi kunda kiberjinoyatlarga qarshish kurashishda O‘zbekiston Respublikasi jiddiy e’tibor qaratmoqda. O‘zbekiston Respublikasi Jinoyat kodeksining XX[1] bobi (Axborot texnologiyalari sohasidagi jinoyatlar)da kiberjinoyatlar uchun javobgarlik belgilangan (278[1]- modda – Axborotlashtirish qoidalarini buzish)[43].

Ammo shu bilan birga, xalqaro standartlar asosida qonunchilikni yanada detallashgan tartibda takomillashtirish zarurati mavjud.
Bunga esa kiberjinoyatlarga oid moddalarning yangilanishi, kiberxavfsizlik masalalariga oid maxsus qonunlarni ishlab chiqish hamda elektron dalillarni to‘plash va saqlash bo‘yicha protsessual qoidalarni takomillashtirish bilan erishiladi.

Shuningdek, kiberjinoyatlarga qarshi kurashish borasida O‘zbekistonda quyidagi muammolar mavjud:

- kiberjinoyatlar bilan bog‘liq milliy qonunchilikning ba’zi jihatlari xalqaro standartlarga to‘liq mos kelmasligi;
- kiberjinoyatlarga oid sud amaliyotining yetarlicha rivojlanmaganligi;
- kadrlar yetishmasligi va texnik imkoniyatlarning cheklanganligi.

Mazkur muammolarni bartaraf etish uchun Budapesht konvensiyasiga to‘liq qo‘shilish masalasini imkon qadar tezroq hal etish, kadrlar tayyorlash dasturlarini qayta ko‘rib chiqish hamda xalqaro tajriba almashishni samarali yo‘lga qo‘yish lozim.

[43] O‘zbekiston Respublikasi Jinoyat kodeksi

Budapesht konvensiyasiga qo‘shilish xalqaro hamkorlikni mustahkamlash va milliy qonunchilikni rivojlantirishga yordam beradi, kiberjinoyatlarga qarshi kurash bo‘yicha mutaxassislar tayyorlashda aniq, dolzarb mavzularni tashkil etish faoliyatning rivojlanishiga olib keladi, boshqa davlarlarning kiberjinoyatlar bilan kurashdagi ilg‘or tajribasini o‘rganish milliy qonunchilikdagi huquqiy hamda sohadagi amaliy bo‘shliqlarni to‘ldirishga zamin yaratadi**.**

Xulosa qilib aytganda, kiberjinoyatlarga qarshi kurashda xalqaro kelishuvlar va milliy qonunchilikning o‘zaro uyg‘unligi hal qiluvchi ahamiyatga ega. O‘zbekistonning bu boradagi harakatlari, xususan, Budapesht konvensiyasiga qo‘shilish jarayoni, kiberjinoyatchilikning oldini olish va ularni nazorat qilishda yangi imkoniyatlarni ochib beradi. Shu bilan birga, milliy qonunchilikni xalqaro standartlarga moslashtirish va davlatlararo hamkorlikni kuchaytirish ustuvor yo‘nalish sifatida davom ettirilishi lozim.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. O‘zbekiston Respublikasi Jinoyat kodeksi;
2. O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni;
3. 2001-yildagi 23-noyabrdagi Yevropa Kengashi, “Budapest konvensiyasi”
4. https://akadmvd.uz.
5. “Kiberjinoyatchilikka qarshi immunitet hosil qilish masalalari” B.O.Primov / Ilmiy maqola;
6. https://cyberleninka.ru.

ИЧКИ ИШЛАР ОРГАНЛАРИНИНГ ЎЗИНИ ЎЗИ БОШҚАРИШ ОРГАНЛАРИ БИЛАН ҲАМКОРЛИГИ ЖАРАЁНИДАГИ ЎЗАРО АХБОРОТ АЛМАШИШ ШАКЛ ВА УСУЛЛАРИ

М.И.Суванкулов

Ахборот ижтимоий ҳаётнинг барча соҳаларида пешқадамлик қилмоқда ва жамиятнинг технологик тараққиёти даврида ҳукм сурадиган «ахборот хокимияти» вужудга келди, шу сабали XXI аср ахборот асри деб аталди.

Агар ахборот алмашинуви ҳодисасига кенг кўламда қарасак, унинг инсон ва жамият ҳаётида нечоғлик катта аҳамиятга эгалигига гувоҳ бўламиз. Социумнинг энг кичик элементи – индивиддан тортиб, инсоният жамиятигача, яъни барчасининг мавжудлик ва ривожланиш шарти ахборот алмашинувидир[44].

Ахборот алмашинуви – ҳамкорлик субъектлари бўлган ички органлари ва фуқароларнинг ўзини ўзи бошқариш органлари ўртасида жамоат тартибини сақлаш, жамоат хавфсизлигини таъминлаш ва ҳуқуқбузарликлар профилактикасига оид бўлган маълумотлар ва ахборотларни ўзаро узатиш борасидаги фаолият ҳисобланади.

[44] Ш.Рахимова. Ахборотлашган жамиятда ахборот алмашинувининг ўзига хос хусусиятлари. INFOLIB AXBOROT-KUTUBXONA JURNAL / https://einfolib.uz/post/ahborotlashgan-jamiyatda-ahborot-almashinuvining-uziga-hos-hususiyatlari

Ўзаро ахборот алмашинув жараёнлари ҳамкорликнинг асосини ташкил қилади, негаки ҳамкорликнинг сақланиб қолинишини маҳаллада хавфсиз муҳитни таъминлашга оид ахборот ва маълумотларни томонларга узлуксиз келиб туриши билангина изоҳлаш мумкин, яъни ички ишлар органлари фуқароларнинг ўзини ўзи бошқариш органларига, ўз навбатида эса фуқароларнинг ўзини ўзи бошқариш органлари ички ишлар органларига ўзларида мавжуд бўлган ахборотларни алмашиб туриши лозим бўлади. Фақтгина ҳар қандай ахборат алмашинуви эмас, балки, ижтимоий фойдали, ҳамкорликка хизмат қилувчи, маҳаллада хавфсиз муҳитни таъминлашга оид бўлган ахборотларгина талаб этилади. Ахборот алмашинувдан ҳам ички ишлар органлари, ҳам фуқароларнинг ўзини ўзи бошқариш органлари манфаатдордир. Ҳар икала субъект ҳам маҳалладаги криминоген вазиятдан бохабар бўлсагина, олиб борилаётган профилактик чора-тадбирлар самарали равишда ташкил этилади, маълумот ва ахборотга эга бўлмасдан туриб муайян ишларни амалга ошириш, айниқса жиноятчиликни жиловлашда албатта ҳар иккала субъект ҳам қийинчиликка дуч келади.

Зеро, фуқароларнинг ўзини ўзи бошқариш органлари жамоатчилик назорати субъекти сифатида Ўзбекистон Республикасининг 2018 йил 12 апрелдаги 474-сонли “Жамоатчилик назорати тўғрисида”ги[45] қонунининг 6-моддасида ҳам жамоатчилик назоратининг шаклларидан бири сифатида жамоатчилик эшитуви ва фуқароларнинг ўзини ўзи бошқариш органлари томонидан давлат органлари мансабдор шахсларининг ҳисоботлари ва ахборотини эшитиш масалалари назарда тутилган.

Шунингдек, Ўзбекистон Республикасининг 2016 йил 16 сентябрдаги “Ички ишлар органлари тўғрисида”ги[46] қонуннинг 11-моддасига кўра ички ишлар органлари ўз зиммасига юклатилган вазифаларни бажариш мақсадида, қонунчиликда белгиланган тартибда давлат органлари, фуқароларнинг ўзини ўзи бошқариш органлари ва бошқа ташкилотлар билан ҳамкорлик қилади ҳамда аниқланган жиноятлар ва бошқа ҳуқуқбузарликларга оид мавжуд материаллар тўғрисидаги ахборотни алмашишни, шу жумладан электрон шаклда алмашишни, шунингдек бошқа ахборотни алмашишни амалга оширади.

Таҳлиллар натижасидан келиб чиққан ҳолда ички ишлар органлари ва фуқароларнинг ўзини ўзи бошқариш органлари ўртасидаги ахборот алмашинувининг ҳам қуйидаги шаклларга таснифлаган ҳолда ўрганиш мақсадга мувофиқдир.

1) *Ҳужжатлар орқали ахборот алмашиш.* Ички ишлар органлари ва фуқаролар ўзини ўзи бошқариш органлари ўзаро ҳамкорлик жараёнида ҳужжатлар орқали ахборот амашинувини амалга оширади, жумладан фуқароларнинг ўзини ўзи бошқариш органлари маҳаллада истиқомат қилувчи ғайриижтимоий хулқ-атворга эга бўлган, ҳуқуқбузарлик содир этишга мойил бўлган, гиёҳвандлик, психотроп ва инсон ақлига салбий таъсир кўрсатувчи моддаларни истеъмол қилувчи, спиртли ичимликка ружў қўйган шахслар,

[45] Қонун ҳужжатлари маълумотлари миллий базаси, 13.04.2018 й., 03/18/474/1062-сон;
[46] збекистон Республикаси қонун ҳужжатлари тўплами, 2016 й., 38-сон, 438-модда

рўйхатдан ўтмасдан яшаб келаётган фуқаролар, ноқонуний фаолият билан шуғулланётган тадбиркорлар, ноқонуний диний ўқиш ташкил қилинган хонадонлар, низоли оилалар ҳамда бошқа турдаги маълумотларни ички органларига мурожаатни ёзма шаклда, яъни *ариза* ва *шикоят* шаклида, шунингдек маҳаллада жиноятчиликни олдини олишга оид амалга оширилиши лозим бўлган чора-тадбирларга доир тавсияларни ўз ичига олган *таклиф* шаклида мурожаат қилади, айрим ҳолларда ўтказилган ишлар хусусидаги маълумотни *баённома* ёки *далолатнома* шаклида ҳам тақдим этади, шунингдек ички ишлар органларининг сўровномаларига асосан *маълумотнома* шаклида тақдим қилса, ички ишлар органлари эса ҳудуддаги жиноятчиликнинг умумий аҳволи хусусидаги *статистик маълумотлар*, кунлик содир бўлган жиноятлар ҳақида *хабар*, маҳалла ҳудудида содир бўлган катта шов-шувга сабаб бўлган жиноятлар бўйича олиб борилаётган терговга қадар текширув ва суриштирув ишлари хусусида жамоатчиликни бохабар қилиш мақсадида *маълумотнома* тақдим қилиш, “хавфсиз маҳалла”, “хавфсиз хонадон” тамойили асосида ички ишлар органлари томонидан олиб борилаётган профилактик чора-тадбирлар бўйича эса *таҳлилий маълумот, ахборот хати* ва *ҳисобот* шаклида ёзма ҳужжатлар тақдим қилиш йўли билан ахборот алмашинуви орқали ҳамкорликни ташкил қилади.

2) *Мобил алоқа воситалари ёрдамида ахборот алмашиш*. Ҳозирги пайтда ахборот алмашинуви жаҳондаги глобаллашув ахборотлашган цивилизация шаклланишининг таркибий қисми сифатида аввалги замон шароитидан бутунлай фарқ қилади. Жамиятнинг технологик тараққиёти даврида ёзма ахборот ўрнини мобил алоқа воситалари ёрдамида ахборот алмашинуви эгаллаётганлиги ҳеч кимга сир эмас. Мобил алоқа охирги йилларда кундалик ҳаётимизга кириб келиб, кун сайин унда мустаҳкам ўрнашиб олмоқдаки, у бўлмаса ҳозирги замон жамиятини тассавур қилиш мураккаб бўлиб қолмоқда.

Жиноятчилик билан курашиш амалиётининг ривожланиши, хавфсизлик ва жамоат тартибини таъминлаш – ички ишлар органлари олдида турган вазифаларни муваффақиятли бажариш, аксарият ҳолатларда улар фаолиятининг ахборот ва таҳлилий таъминланганлик даражаси билан белгиланишини кўрсатади.

Фаолиятга мобил алоқа воситаларидан фойдаланиш жараёнидаги катта ҳажмдаги маълумотлар билан ишлар юкини енгилаштиришга ёрдам берган ҳолатларда айниқса асқотади. Бу ўз ўрнида, иш жараёнида вақтнинг тежалишига, вазифаларни бажариш сифати ва тезкорлигининг ошишига ёрдам беради.

Хусусан, ички ишлар органлари ва фуқароларнинг ўзини ўзи бошқариш органлари ўртасидаги мобил алоқа воситалари орқали ахборот алмашинуви ҳам муҳим ўринни эгаллайди десак муболаға бўлмайди. “Хавфсиз маҳалла” тамойили асосида маҳалла ҳудудида жамоат тартибини сақлаш ва жамоат хавфсизлигини таъминлаш борасида амалга оширилаётган ҳамкорлик жараёнида ички ишлар органлари ходимлари, айниқса профилактика инспекторлари бириктирилган ҳудуддаги маҳалладаги оператив вазиятни аниқлаш ва ундан бохабар бўлиб туриш учун кундалик равишда маҳалла раиси билан уяли алоқа восита орқали маҳалладаги вазият хусусида маълумот олиш амалиёти йўлга

қўйилган. Профилактика инспектори ҳудудида бўлиши ёки иш юзасидан бошқа ҳудудга ёки давлат ташкилотига кетган вақтида маҳаллада содир бўлган ҳуқуқбузарлик ёки жиноят хусусида маҳалла раисидан ёки фуқаролардан содир этилган жиноят юзасидан бирламчи маълумотларни сўраб олиши, ёки аксинча профилактика инспектори маҳалла ҳудудида бўлмаган тақдирда содир этилган жиноят ёки ҳуқуқбузарлик хусусида маҳалла раиси томонидан хабардор қилиниши, шунингдек қидирувда юрган шахс ҳақида маълумотларни зудлик билан олишда, ёки оилавий низолар, спиртли ичимликка ружъу қўйган шахс томонидан содир этилаётган безорилик ва шунга ўхшаш маълумотлардан тезкорлик билан воқиф бўлишда мобил алоқа воситаси орқали маълумот олиш ва олинган маълумот хусусида ички ишлар органлари раҳбарияти ёки бошқа масъул мансабдор шахсларни хабардор қилиши, воқеа жойига керакли куч ва воситаларни жалб қилишда фойдаланади. Ҳамкорликнинг мобил алоқа восита орқали ахборот олиш шакли ҳозирги кундаги энг қулай, тезкор ва мақбул шакли ҳисобланади.

3. «Telegram» мессенжерлар орқали ахборот алмашиш. Ички ишлар органлари ходимлари зиммасига юрт тинчлиги ва осойишталигини таъминлашдек масъулиятли ва шарафли вазифа юкланган бўлиб, аҳолига ўз вақтида ва сифатли ёрдам кўрсатадиган, халқ манфаатларига хизмат қиладиган профессионал, халқчил тузилмага айлантириш бўйича кенг кўламли чора-тадбирлар олиб борилмоқда.

Бугунги кунда турли хавф-хатар ва таҳдидлар, халқаро терроризм ва экстремизм, коррупция, гиёҳвандлик, одам савдоси, ноқонуний миграция, ахборот хуружи ва ёт ғояларга қарши курашиш, уларга барҳам бериш бўйича ички ишлар органлари олдига янги вазифалар қўйилди.

Янги технологияларнинг ривожланиши ижтимоий ҳаётнинг ўзига хос ижобий ўзгаришига олиб келади. Ахборотлашган жамиятда ахборот алмашинувида ахборотни ташувчиси ижтимоий тармоқ *«Telegram»* мессенжерининг ўрни муҳим.

“Telegram” месенжери ҳақидаги https://uz.tgstat.com/ сайтининг берган маълумотига кўра, Ўзбекистон каналлар сони бўйича Россия, Эрон, Ҳиндистон давлатларидан кейин тўртинчи ўринга чиқиб олган, ҳозирда Ўзбекистонда Telegram каналларининг умумий аудиторияси 956.000.000 тани ташкил қилади, 153 мингдан ортиқ Telegram канали ва 27 мингга яқин чат борлиги[47], ахборот ташувчи сифатида Telegram каналининг ўрни нечоғлик даражада аҳамиятлига шубҳа йўқ.

“Хавфсиз маҳалла” тамойили асосида маҳалла кесимида жиноятчиликни жиловлашда ички ишлар органлари ва фуқаролар ўзини ўзи бошқариш органларининг ахборот алмашишда Telegram каналидан фойдаланиш жуда қулай, тезкор ва арзон воситадир.

Ҳаммамизга маълумки ҳозирги кунда барча маҳалалларда маҳалланинг телеграм канали очилган ва фуқаролар ушбу каналларга аъзо бўлган, шу

[47] https://uz.tgstat.com/

жумладан каналнинг администратори маҳалла раиси, маҳалла профилактика инспектори эса аъзоси ҳисобланади.

Телеграм каналидан профилактика инспектори ва маҳалла раиси қуйидаги шаклларда фойдаланади:

Биринчидан, телеграм каналларга фуқаролар маҳаллада содир этилган ножўя ҳаракатлардан хабардор бўлиш орқали маълумотлар олинади, ушбу маълумотлар текширилиб, маҳалла раиси ва профилактика инспектори томонидан тегишли чора-тадбирлар амалга оширилади.

Иккинчидан, маҳаллада ўтказилиши режалаштирилаётган профилактик чора тадбирлар, хусусан "жиноятлар муҳокамаси", "ҳуқуқий тарғибот соатлари", ёшлар ўртасидаги "спорт мусобоқалари", "оммавий ҳашарлар" ва бошқа тадбирлар хусусида маҳалла аҳолиси хабардор қилинади;

Учинчидан, маҳаллада содир этилган жиноятларни иссиқ изидан очиш мақсадида телеграм канал орқали жиноят тафсилотлари ва гумонланувчилар хусусида маълумотлар тўпланади, яъни ҳар бир фуқаро билан якка тартибда сўров ўтказишдек катта ҳажмли ишлар қисқа муддатда ва енгил шаклда бажарилади.

Тўртинчидан, қидирувдаги шахслар хусусидаги маълумотлар, олиб қочилган автотранспорт воситалари, йўқолган ҳужжатлар, гумонланувчи шахсни шахсини аниқлаш хусусидаги маълумотлар телеграм ижтимоий таромғи орқали юборилиб, фуқаролардан маҳалла раиси орқали маълумотлар йиғиб олинади.

Бешинчидан, маҳалла раиси ва профилактика инспектори бир-бирига ҳамкорликка оид тадбирлар режаси, ижтимоий профилактик хулосалар, бажарилган ишлар бўйича маълумотларни фотожамланмаси билан бирга юборади.

Олтинчидан, маҳалла аҳолисини ҳуқуқий онги ва маданиятини, ҳуқуқий саводхонлигини ошириш мақсадида янги қабул қилинган қонун ва қонун ости ҳужжатларидан хабардор қилиб туради;

Еттинчидан, сайлов ва референдум ҳақида маълумотларни аҳолига ҳамкорликда телеграм орқали етказади ва бошқа шу сингари ахборот алмашинуви амалга оширилади.

4. Ахборот базалари орқали ахборот алмашиш.

Рақамли технологиялар соҳасида амалга оширилаётган ислоҳотлар натижасида ички ишлар органлари соҳасида ҳам тизим фаолиятини рақамлаштириш, давлат органлари ва ташкилотлар (шунингдек фуқаролар) билан реал вақт режимида ахборот алмашинувини таъминлаш, қоғозбозликни олдини олишга қаратилган, айниқса, аҳолига кўрсатиладиган давлат хизматларини тезкорлик билан ижросини таъминлаш мақсадида ахборот тизимлари яратилди ва бу жараён изчил давом эттирилмоқда.

Сўнгги маълумотларга кўра, ички ишлар органларида ҳозирги кунда 70 га яқин ахборот тизимлари фаолияти йўлга қўйилган. Соҳавий хизматлар кесимида таҳлил қилинганда, Миграция ва фуқароликни расмийлаштириш хизматида 9 та, Ҳуқуқий статистика ва тезкор-ҳисоб маълумотлар марказида 6 та, Эксперт-криминалистика бош марказида 6 та, йўл ҳаракати хавфсизлиги

хизматида 6 та, жазони ижро этиш хизматида 8 та, Ташкилий департаментда 1 та, Ҳуқуқбузарликлар профилактикаси хизматида 5 та ва бошқа хизматларда 10 га яқин интеграциялашган ахборот тизимлари мавжуд.

Аҳоли билан энг кўп мулоқотда бўлувчи профилактика хизмати фаолиятида ахборот алмашинувини рақамлаштириш мақсадида қуйидаги интеграциялашган ахборот тизимлари ишлаб чиқилган:

“Smart mahalla” Android 5.0 ва ундан юқори версиядаги операцион тизимда ишловчи мобил қурилмалар (смартфон, планшет ва бошқалар) учун мўлжалланган мобил илова бўлиб, ушбу ахборот тизимида фуқаролар, яъни кенг жамоатчилик учун ўзининг яшаб турган ҳудуди (туман, шаҳар, вилоят), маҳалласи, жамики бутун республика бўйича хавфсиз муҳитни таъминлашга қаратилган маълумотларни олиш имконияти яратилган. Шунингдек, “Smart mahalla” ахборот тизимидан профилактика инспекторига масофадан туриб мурожаат юбориш ва уни кўриб чиқиш жараёнини кузатиб бориш, аҳоли билан ўзаро тезкор мулоқотни йўлга қўйиш, профилактика инспекторлари ва сектор раҳбарлар фаолиятига баҳо бериш имконини берувчи қулайлик яратилган. *(ахборот тизими ҳозирда қайта ишланиб, такомиллаштирилмоқда)*.

«E-jamoat xavfsizligi» ягона автоматлаштирилган ахборот тизими – Миллий гвардия ва ички ишлар органларидан жамоат тартибини сақлашга жалб қилинган бўлинмаларнинг ахборот тизимлари (пробациянинг марказлашган электрон тизими, йўл ҳаракати хавфсизлиги хизматининг ягона автоматлаштирилган ахборот-таҳлил тизими) базасида ишлаб чиқилган бўлиб, Ўзбекистон Республикаси Президентининг 2021 йил 29 ноябрдаги “Ўзбекистон Республикаси жамоат хавфсизлиги концепциясини тасдиқлаш ва уни амалга ошириш чора-тадбирлари тўғрисида”ги ПФ-27-сон Фармони[48] асосида яратилган. Мазкур ахборот тизими жамоат хавфсизлигини таъминлаш йўналишидаги ишларни «Халқ манфаатларига хизмат қилиш» тамойили асосида ташкил этишнинг мутлақо янги механизм ва тартиблари жорий этилишида ҳамда давлат органларининг жамоатчилик тузилмалари билан ўзаро мақсадли ҳамкорлиги йўлга қўйилишига сабаб бўлди.

“E-muhokama” (ахборот тизими) электрон дастури Ўзбекистон Республикаси Президентининг 2023 йил 24 май кунидаги “Рақамли хизматлар қамрови ва сифатини ошириш ҳамда соҳа, тармоқ ва ҳудудларни рақамли трансформация қилиш чора-тадбирлари тўғрисида”ги ПҚ-162-сонли Қарори[49] асосида ишлаб чиқилган. Ушбу электрон дастур орқали муҳокама ўтказиладиган ҳудуд манзили, муҳокама ўтказиладиган сана, сектор раҳбарининг муҳокама жараёни, гумонланувчи яшаш манзили ва жиноят содир этилган вақти, содир этилган жиноят моддаси ва унинг ҳуқуқий оқибатлари ҳақида ахборот-маълумот алмашинуви таъминланади.

“Onlayn-mahalla” ахборот тизими Ўзбекистон Республикаси Президентининг 2021 йил 24 декабрдаги “Иқтисодий тараққиёт ва камбағалликни қисқартириш вазирлиги ҳузуридаги Маҳаллабай ишлаш ва

[48] Қонунчилик маълумотлари миллий базаси, 01.12.2021 й., 06/21/27/1116-сон

[49] Қонунчилик маълумотлари миллий базаси, 25.05.2023 й., 07/23/162/0295-сон;

тадбиркорликни ривожлантириш агентлиги фаолиятини ташкил этиш чора-тадбирлари тўғрисида” ПҚ-62-сон Қарорига[50] мувофиқ ишлаб чиқилган. Мазкур электрон платформа республика миқёсидаги барча ҳоким ёрдамчилари, республика вакиллари, туман марказлари ва туман ҳокимликлари, ҳудудий бошқарма ва вилоят ҳокимликларнинг фаолиятини тўлиқ рақамлаштириш вазифасини бажаради.

Хулоса сифатида шуни айтиш мумкинки, ички ишлар органларининг ўзини ўзи бошқариш органлари билан ўзаро ахборот алмашиш шакл ва усуллари турли хил бўлиб, мазкур ахборот алмашиш орқали жиноятчилик жиловланади, жамоат хавфсизлиги таъминлади, жамоат тартиби сақланади, қолаверса маҳаллада истиқомат қилувчи фуқаролар учун “хавфсиз маҳалла” муҳитини яратишга эришилади.

АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА ХАВФСИЗЛИГИ СОҲАСИДАГИ ЖИНОЯТЛАРНИНГ ОЛДИНИ ОЛИШНИНГ ЎЗИГА ХОС ХУСУСИЯТЛАРИ

Убайдуллаев Шерзод Музаффарович

Ўзбекистон Республикаси ИИВ Малака ошириш институти Касбий тайёргарлик факулътети махсус фанлар цикли ўқитувчиси
+998909569593

Глобал тараққиёт шароитида ахборот технологиялари моҳиятини оширишнинг янада замонавий, инновацион усулларини излаб топиш, ахборотлаштириш жараёнига ҳар томонлама кўмаклашиш, уларни ҳаётга кенг жорий этиш давлат фаолиятининг муҳим йўналишларидан бирига айланмоқда. Зеро, ахборотлаштириш тизимида давлат сиёсатини олиб бориш масаласи стратегик аҳамиятга эга вазифадир[51].

Дунёда ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятчиликка қарши курашиш муаммолари тобора глобал аҳамият касб этмоқда. Ҳусусан БМТ Бош Ассамблеяси, Европа кенгаши, ШҲТ, МДҲ, Араб давлатлари лигаси ва бошқа ташкилотлар томонидан ахборот-коммуникатсия технологияларидан жиноий мақсадларда фойдаланишга қарши курашиш бўйича ҳалқаро ҳуқуқий ҳужжатлар қабул қилинган. Статистик маълумотларга кўра, ҳозирги вақтда **7 миллиардга** яқин инсон (дунё аҳолисининг 95%) электр алоқасининг кўчма тармоқлари билан қамраб олинган[52], йилига кибержиноятчилик оқибатида етказилган моддий зарарнинг миқдори дунё ЯИМнинг **1 %ни** ташкил этади[53].

---

[50] Қонунчилик маълумотлари миллий базаси, 10.02.2024 й., 07/24/62/0110-сон

[51] Х.Б. *Абдреймов* Ахборот технологиялари соҳасидаги жиноятлар ва улардан ҳимояланиш усуллари *ИИВ Академия Магистратура ингловчиси.*

[52] Расулев А. К. Ахбороттехнологияларивахавфсизлигисоҳасидаги жиноятларга қарши курашишнинг жиноят-ҳуқуқий ва криминологик чораларини такомиллаштириш. Юрид. фанлар доктори диссертациясининг автореферати. Т., ИИВ Академияси, 2018. - Б-5.

[53]. http://www.statista.com/The StatisticsPortal).

Янгидан-янги турлари билан тилга олинадиган кибержиноятчиликнинг ижтимоий ҳаётимизга кириб келганига ҳам анча бўлди ва уни асримизнинг глобал муаммолари қаторига қўшимиз мумкин. Унинг бизга маълум бўлган вирусли дастурларни тарқатиш, паролларни бузиб кириш, кредит карта ва бошқа банк реквизитларидаги маблағларни ўзлаштириш талон-тарож қилиш, шунингдек Интернет орқали қонунга зид ахборотлар, хусусан бўҳтон, маънавий бузуқ маълумотларни тарқатиш билан башарият ҳаётига катта хавф солаётганидан кўз юмиб бўлмайди.

Интернет (инг. Интернет) – ахборотни сақлаш ва узатиш учун мўлжалланган бутунжаҳон умумлаштирилган компютер тўридир. Кўпинча “Умумжаҳон тўри” ёки “Глобал тўр” деб номланади. Унинг асосида “Бутунжаҳон ўргимчак тўри” (Ворлд Виде Веб, WWW) ва бошқа алоқа системалари фаолият юритади.

Ҳозир бутун дунёдаги инсониятнинг 63 фоизи интернетдан фойдаланади. Қарийб бир йилда интернет фойдаланувчилари сони 200 миллионга ортган. Фойдаланувчиларнинг асосий қисми **(92,4 фоиз)** мобил қурилмалар орқали интернетдан фойдаланади. Ўзбекистонда интернет фойдаланувчилари сони **27 миллиондан** ошган, шундан **25 миллиондан** кўпроғи мобил интернет фойдаланувчилари ҳисобланишади[54].

Ахборот технологияларининг кенг миқёсда ривожланиши бир вақтнинг ўзида кўп турдаги жиноятларнинг содир этилишига имкон яратди, ўз навбатида ушбу турдаги жиноятларни аниқлаш ва уларни олдини олишда юқори билим ва касбий тайёргарликни талаб қилмоқда. Шундай қилиб, “ахборот технологиялари соҳасидаги жиноят” компютерлар ва маълумотларни қайта ишлаш тизимларидан фойдаланган ҳолда содир этиладиган жиноий қилмиш бўлиб, бунинг учун қонунчиликда жиноий жавобгарлик назарда тутилган. Шу боис, фуқаролар ўртасида ахборот технологиялари соҳасидаги жиноятлар тўғрисида маълумотларни тарқатиш ва тарғибот-ташвиқот ишларини олиб бориш зарур.

Ахборотлашган жамият тезлик билан шаклланиб, ахборот дунёсида давлат чегаралари деган тушунча йўқолиб бормоқда. Жаҳон компютер тармоғи давлат бошқарувини тубдан ўзгартирмоқда.

Ҳудудий жойлашишидан қатъий назар, кундалик ҳаётимизга турли хилдаги ахборотлар интернет халқаро компютер тармоғи орқали кириб келади. Шунинг учун ҳам мавжуд ахборотлардан ноқонуний фойдаланиш, ўзгартириш, йўқотиш ва уларга кириш каби муаммолардан ҳимоя қилиш долзарб масала бўлиб қолди.

Маълумотларга кўра, дунё бўйлаб ҳар йили **500 миллиондан** ортиқ киберҳужумлар уюштирилади. Ҳар сонияда дунёдаги ҳар **12 нафар** инсондан бири кибермаконда содир этилган ҳужумлар қурбонига айланмоқда. Хусусан, АҚШ, Франсия, Англия, Белгия, Германия, Луксембург каби давлатларда кибержиноятчилик кўрсаткичи умумий жиноятчиликнинг **60–65 фоизини** ташкил этади.

[54] https://review.uz/oz/post/ozbekistonda-internet-xizmatidan-foydalanuvchilar-soni-272-milliondan-oshdi

Экспертларнинг ҳисоб-китобича, киберҳужумларнинг асосий қисми махфий маълумотларни қўлга киритиш, уларни ўзгартириш ёки йўқотиш, фойдаланувчилардан пул талаб қилиш ёки бизнес жараёнларини издан чиқаришга қаратилмоқда. Бунинг натижасида бир йилда дунё иқтисодиёти ўртача **20 миллиард** АҚШ долларидан зиёд миқдорда зарар кўрмоқда.

Ўзбекистонда ҳам сўнгги уч йилда кибержиноятлар **8,3 бараварга** кўпайиб, умумий жиноятчиликнинг **5 фоизини** ташкил этмоқда. Масалан, кибермаконда фирибгарлик билан боғлиқ ҳолатлар **13 бараварга,** ўғрилик **20 бараварга,** товламачилик, туҳмат ва ҳақорат қилиш билан боғлиқ жиноятлар эса **4,9 бараварга** ортган.

Жиноий-ҳуқуқий тушунчада компютер ахбороти ахборот технологиялари соҳасидаги жиноятларнинг предмети ҳисобланади. Масалан бундай ҳолатлар Жиноят кодекси 2781, 2782, 2784, 2786 ва 2787-моддаларининг диспозитсияларида тўғридан-тўғри кўрсатилган. Бошқа ҳолларда эса предметнинг аниқланиши жиноят таркиби бошқа элементларининг аниқланиши билан боғлиқ (ЖКнинг 2783 ва 2785-моддалари).

Ўзбекистон Республикаси Жиноят кодекси Махсус қисмининг ахборот технологиялари соҳасидаги жиноятларга оид бобининг хусусияти шундаки, унда ахборотнинг алоҳида тури – компютер ахбороти ҳақида сўз боради.

Юқоридагилардан келиб чиққан ҳолда таъкидлаш мумкинки, ушбу турдаги жиноятлар ахборот технологияларидан қонуний, хавфсиз фойдаланишни таъминловчи муносабатларга бевосита тажовуз қилади ҳамда фойдаланувчиларнинг ахборот технологиялари соҳасидаги қонуний манфаатларига зарар етказади.

Ахборот технологиялари соҳасидаги жиноятларнинг олдини олишда қуйидагиларга алоҳида эътибор қаратиш таклиф этилади:

биринчидан, Ўзбекистон Республикаси Жиноят кодексининг 168-моддаси 2-қисми “в” бандини “телекоммуникатсия тармоқларидан, шунингдек, Интернет жаҳон ахборот тармоғидан ёки электрон тўлов воситаларидан фойдаланиб” тарзида баён этиш, 273-моддаси 2-қисмини “телекоммуникатсия тармоқларидан, шунингдек Интернет жаҳон ахборот тармоғидан фойдаланиб содир этилган бўлса” таҳриридаги янги “д” банди билан тўлдириш.

Содир этилаётган фирибгарлик жиноятлари таҳлил қилинганида, аксарият бу турдаги жиноятлар ахборот технологияларидан фойдаланган ҳолда, айниқса, мобил иловалар орқали банк пластик карталаридан пулларни фирибгарлик ва ўғрилик қилиш орқали ўзлаштириш ҳолатлари кўпаймоқда.

Амалдаги Жиноят кодексининг 168-моддаси 2-қисми “в” бандида ёки 169-моддаси 3-қисми “б” бандида компютер техникасидан фойдаланиб содир этилган фирибгарлик ва ўғрилик жиноятлари учун жавобгарлик белгиланган. Бироқ “Компютер техникасидан фойдаланиб содир этиш” тушунчаси тор маънода бўлиб, ҳозирда бу турдаги жиноятларнинг содир этиш усулини тўлиқ қамраб олмаяпти.

Қолаверса, мазкур моддани шу йўналишда 2022 йил 15 апрелда қабул қилинган “Киберхавфсизлик тўғрисида”ги Қонун талабларига мослаштириш лозим.

Таклиф этилаётган *“Телекоммуникатсия тармоқларидан, шунингдек Интернет жаҳон ахборот тармоғидан ёки электрон тўлов тизимларидан фойдаланиб”* жумласи Россия Федератсияси Жиноят кодексининг 159.6-моддасида ўз аксини топган бўлиб, ушбу қилмиш учун алоҳида жиноий жавобгарлик белгиланган. Бундан ташқари, Россия Федератсияси Жиноят кодексининг 159.3.-моддасида электрон тўлов воситаларидан фойдаланиб содир этилган фирибгарлик учун алоҳида жиноий жавобгарлик белгиланган.

Шунингдек, Украина Жиноят кодексининг 190-моддасида, Латвия Жиноят кодексининг 177.1-моддасида қонунга хилоф равишда электрон ҳисоблаш машинаси техникасидан фойдаланганлик ва автомат тизимида маълумотларга ишлов беришда фирибгарлик содир этганлик учун махсус жиноий жавобгарлик белгиланган;

иккинчидан, мобил илова аккаунтини фаоллаштиришда (телефон аппаратининг ИМЕИ коди, ИП-манзиллар рўйхатидан ташқари) фойдаланувчининг юз кўриниши (Фасе ИД), географик жойлашув (геопозитсия - Лосатион) маълумотларини тўлиқ киритишга доир техник шартни жорий этиш.

Маълумот учун: 2017 йилда Россиядаги “Сбербанк” ҳамда “Точка” номли мобил иловаларида “Фасе ИД”, “Лосатион” функсиясининг жорий этилиши улар билан боғлиқ жиноятларнинг **85 %**га камайишига олиб келган. Мазкур амалиётнинг йўлга қўйилиши мобил иловалар орқали содир қилинаётган жиноятларнинг камайишига, жиноятни содир қилган шахс ҳамда жойлашган манзили ҳақидаги маълумотларни ўз вақтида аниқлашга, молия хизматларини кўрсатиш субъектлари ҳамда дастурий таъминотдаги хавфсизлик даражаси яхшиланишига, фуқароларнинг пластик карталаридаги маблағлари ишончли муҳофаза қилиниши таъминланишига хизмат қилади;

учинчидан, “Ропулатион оф Узбекистан” ахборот-қидирув-маълумотнома тизимини жорий қилиш ва бунда сунъий интеллект технологиялари имкониятларидан кенг фойдаланиш.

Дунёнинг етакчи давлатлари (Италия, АҚШ ва ҳ.к.) тажрибасига кўра, мамлакат аҳолисининг ҳар бирининг туғилганидан бошлаб вафот этгунига қадар барча жараён, жумладан боғчада, мактабда (литсей, коллеж, техникум ва ҳ.к.), олий таълим муассасасида таълим олиш ва иш жойидаги меҳнат қилиш жараёнларида унинг феъл-атвори, қизиқиши, атрофидаги инсонлари, оилавий аҳволи ва ҳ.к. маълумотлари доимий ва мунтазам тўлдирилиб бориладиган, марказлаштирилган, рухсат даражалари белгиланган “Ропулатион оф Узбекистан” ахборот-қидирув-маълумотнома тизимини жорий қилиш ва бунда сунъий интеллект технологиялари имкониятларидан кенг фойдаланиш таклиф этилади. Бу тизим мамлакатимиз аҳолиси тўғрисида барча маълумотларни жамлаганлиги сабаб жиноятларни “иссиқ изи”дан очиш ҳар бир криминал вазиятда аниқ ва тўғри қарорлар қабул қилиш учун хизмат қилади. Мазкур тизимнинг ички ишлар тизимларига жорий қилинаётган рақамли технологиялар билан интегратсиялашуви бугунги кунда жиноятларни жиловлаш учун энг катта самара берадиган тадбирлардан бири бўлади;

тўртинчидан, ижтимоий тармоқларда таниқли бўлган блогер, вайнер ҳамда тиктокерлардан кенг фойдаланган ҳолда ахборот технологиялари

соҳасидаги жиноятларнинг олдини олиш бўйича тарғибот-ташвиқот тадбирларини янада кучайтириш.

Сўнгги вақтларда аҳолининг ҳуқуқий маданиятини оширишда, жиноятчиликка қарши курашда ижтимоий тармоқларнинг роли ошиб бормоқда.

Хусусан, айрим блогер, вайнер, тиктокерлар томонидан жамиятнинг барча ижтимоий соҳаларида бўлаётган жараёнларни турли кўринишларда намойиш этишлари миллионлаб фуқаролар томонидан томоша қилиниб, ижтимоий тармоқларда аҳоли орасида муҳокамалар қилинмоқда.

Ҳозирда аҳолининг ҳуқуқий маданиятини оширишда, кибержиноятчиликка қарши курашда блогер, вайнер, тиктокерларнинг хизматларидан фойдаланишни кучайтириш орқали фуқароларни ўзига жалб қиладиган, кўплаб муҳокамаларга сабаб бўладиган ижтимоий роликлар, карикатуралар, видеороликлар, буклетлар, суръатлар ишлаб чиқиш ва уларни аҳоли орасида, айниқса, блогер, вайнер, тиктокерларнинг шахсий профилларида намойиш қилиш мақсадга мувофиқдир.

ЯНГИ ЎЗБЕКИСТОНДА РАҚАМЛИ ИҚТИСОДИЁТ

Убайдуллаев Шерзод Музаффарович

Ўзбекистон Республикаси ИИВ Малака ошириш институти Касбий тайёргарлик факультети махсус фанлар цикли ўқитувчиси

+998909569593

Ҳозирги кунда рақамли иқтисодиётнинг дунё миқёсида тутган ўрни ва унинг ривожланиш тенденциялари тобора ортиб бормоқда. Мисол учун, маълумотлар оқими кўламининг ўзгариши интернет протоколи (IP) га асосланган глобал трафик ҳажмининг 1992 йилда кунига 100 гигабайтни ташкил этган бўлса, 2019 йилда бу кўрсаткич секундига 89000 Гб дан ошди. Бу маълумотлар рақамли иқтисодиёт ривожланишининг дастлабки босқичига тегишли эканини ҳисобга олсак, унинг ривожланиши суръати тўғрисида тасаввур ҳосил қилиш қийин эмас. Прогнозларга кўра, 2022 йилга келиб глобал IP-трафик ҳажми секундига 150700 Гб га етади, бу Интернет тармоғида янги фойдаланувчиларнинг кўпайиши ва Интернетнинг янада кенгайиши натижасида амалга ошади[55]. Жаҳон миқёсида олиб қарайдиган бўлсак, рақамли иқтисодиётнинг ривожланиш географиясида икки мамлакат етакчи ўринни эгаллаб турибди. Булар АҚШ ва Хитой. Бу мамлакатларга блокчейн технологияси билан боғлиқ бўлган барча патентларнинг 75 фоизи, “Internet of Things (Нарсаларинтернети)”га[56] сарфланадиган харажатларнинг 50 фоизи ва булутли ҳисоблаш очиқ технологиялари глобал бозорининг 75 фоизидан ортиғи

[55] 1 БМТ савдо ва ривожланиш конференцияси. Рақамли иқтисодиёт бўйича ҳисобот (2019). https://unctad.org/en/PublicationsLibrary/der2019_overview_ru.pdf

[56] Internet of Things, IoT – қурилмаларни компютер тармоғига бирлаштирадиган ва уларга дастурий таъминот, амалий дастурлар ёки техник воситалардан фойдаланган ҳолда маълумотларни тўплаш, таҳлил қилиш, қайта ишлаш ва бошқа объектларга узатиш имконини берадиган технология.

тўғри келади. Энг диққатга сазовор томони шундаки, улар дунёдаги 70 та энг йирик рақамли платформаларнинг бозор капиталлашувининг 90фоизини назорат қилишади. Технологияларда глобал устунликка интилишнинг оқибатида юзага келади. АҚШ ва Хитойнинг ЯИМ ҳажми бўйича жаҳонда биринчи ва иккинчи ўринларни эгаллаб турганлигини эътиборга олсак, рақамли технологияларнинг мамлакат иқтисодиётини ривожлантиришда стратегик аҳамиятга эга эканлигига яна бир бор ишонч ҳосил қилишмумкин. Ҳозирги пайтда компьютерлаштириш ва юқори технологиялар асрида рақамли иқтисодиёт ҳаётимизнинг ҳар бир жабҳасига: соғлиқни сақлаш, таълим, интернет-банкинг, ҳукуматга дахлдор бўлмоқда. Ўзбекистон Республикаси Президентининг “Рақамли иқтисодиёт ва электрон ҳукуматни кенг жорий этиш чора-тадбирлари тўғрисида”ги 2020 йил 28 апрелдаги, ПҚ-4699-сонли Қарори асосида 2023 йилга келиб рақамли иқтисодиётнинг мамлакат ялпи ички маҳсулотидаги улушини 2 бараварга кўпайтиришни назарда тутилган. Иқтисодиётни ривожлантириш стратегияси саноат, хизмат кўрсатиш соҳаси ва қишлоқ хўжалигини равнақ топтириш, тадбиркорда ташаббускорликни кучайтириш, молиявий ресурслар билан таъминлаш каби омилларга асосланади. Иқтисодиётда чуқур таркибий ўзгаришларни амалга ошириш ҳисобига 2035 йилга бориб, мамлакат ялпи ички маҳсулоти 122 миллиард долларга етказилади. Ўсиш суръатининг бундай кўламини белгилашда ЯИМнинг номинал ўсиши, иқтисодиёт самарадорлиги, аҳоли жон бошига даромадлар ошиши ҳисобга олинган. Ижтимоий соҳани ривожлантириш бўлимида таълим тизими, меҳнат бозори ҳисобига инсон капиталини ривожлантириш, аҳолининг барча қатламларини сифатли тиббий хизмат билан қамраб олиш, илм-фан ва инновацияларни ривожлантириш орқали аҳолининг соғлиғини яхшилаш кўрсаткичларини ошириш, ижтимоий ҳимоя, атроф-муҳитни асраш, илғор фикрлайдиган янги авлодни шакллантириш, мамлакатнинг миллий брендини халқаро миқёсда оммалаштириш каби мақсадлар баён этилган. Ўзбекистонни 2035 йилгача ривожлантириш стратегияси Ҳаракатлар стратегиясининг мантиқий давоми бўлиб, юртимиз тараққиётида янги саҳифа очиши билан аҳамиятлидир. Стратегия лойиҳасида белгиланган марраларга эришиш учун ҳар бир соҳада ислоҳотларни босқичма-босқич, аниқ муддатларда руёбга чиқариш прогнозлари кўрсатилган.

Мамлакатни бугунги кунда демократик, эволюцион йўлдан ривожланиши энг самарали йўл бўлиб, ўзининг самарали натижаларини бермоқда. Бозор иқтисодиёти шароитида ҳамма нарсани талаб ва таклиф белгилайди. Аҳолининг талаб ва таклифини қондириш мақсадида Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги ПФ-60-сонли фармонининг *учунчи устувор йўналишида* **Миллий иқтисодиётни жадал ривожлантириш ва юқори ўсиш суръатларини таъминлаш** доирасида корхоналарнини модернизация қилиш ва жадал ривожлантириш орқали рақамли иқтисодиёт технологияларни жорий этиш бўйича илмий-тадқиқот ишларини кенгайтириш катта аҳамият касб этади. стратегиясини 2035 йилларда амалга оширишда рақамли иқтисодиёт муҳим роль ўйнайди. Ўзбекистон Республикаси Президенти Ш.М.Мирзиёевнинг Олий Мажлисга Мурожаатномасида таъкидлаганидек: “...рақамли иқтисодиётни шакллантириш керакли инфратузилма, кўп маблағ ва

меҳнат ресурсларини талаб этишини жуда яхши биламиз. Бироқ, қанчалик қийин бўлма-син, бу ишга бугун киришмасак, қачон киришамиз?! Эртага жуда кеч бўлади. Шу боис, рақамли иқтисодиётга фаол ўтиш – келгуси 5 йилдаги энг устувор вазифаларимиздан бири бўлади.Рақамли технологиялар нафақат маҳсулот ва хизматлар сифатини оширади, ортиқча харажатларни камайтиради”[57] . Умумжаҳон тенденциялари ва ташқи сиёсатда рўй бераётган ҳодисалардан келиб чиқиб, Ўзбекистон олдида глобал рақобатбардошлик ва миллий хавфсизлик масаласи турибди ва ушбу масалани ҳал қилишда мамлакатда рақамли иқтисодиётни ривожлантириш муҳим роль ўйнайди. Рақамли иқтисодиётнинг айрим элементлари аллақачон муваффақият билан ишламоқда. Ҳозирги кунда, ҳужжатлар ва коммуникацияларнинг оммавий равишда рақамли воситаларга ўтказилишини ҳисобга олиб, электрон имзога рухсат бериш, давлат билан мулоқот қилиш ҳам электрон платформага ўтказилмоқда. Ўзбекистон Республикасининг “Илм-фан ва илмий фаолият тўғрисида”ги 2019 йил 29 октябрдаги 576-сонли қонунига асосан илм-фан ва технологияларни ривожлантиришнинг устувор йўналишлари миллий иқтисодиёт рақобатбардошлиги ҳамда самарадорлигига эришиш, меҳнат унумдорлигини ошириш, янги тармоқларни яратиш, аҳоли турмуш даражаси, илм-фан ва таълим тизимларини сифат жиҳатидан юксалтириб бориш билан боғлиқ муаммоларнинг илмий ечимини таъминлаш мақсадида ишлаб чиқилади[58].

Иқтисодиёт тармоқларида инновация, замонавий техника ва технологиялар қўллашни амалга ошириш учун рақамлм иқтисодиётдан кенг фойдаланиш зарур. Ушбу талабларга жавоб бериш учун “Рақамли иқтисодиёт” фани бўйича чуқур билимга эга бўлиш муҳим аҳамиятга эга. Иқтисодий жараёнларни рақамлаштириш нафақат бевосита ахборткоммуникация тармоғини, балки мамлакат хўжалик фаолиятининг барча соҳаларини ҳам қамраб оладиган кенг қамровли тенденцияга айланиб бормоқда. Интернет-савдо, рақамли қишлоқ хўжалиги, «ақлли» электр-тармоқ тизимлари, учувчисиз транспорт, шахсийлаштирилган соғлиқни сақлашда рақамли иқтисодиёт инқилоби кучли ҳис қилинмоқда. Шу сабабли Ўзбекистон Республикаси Президентининг 2018 йил 22 ноябрда қабул қилинган қарорида таъкидланишича: «Рақамли иқтисодиётни жадал ривожлантириш учун шарт-шароитлар яратиш, давлат бошқаруви тизимини янада такомиллаштириш, ундан фойдаланиш имкониятларини кенгайтириш, замонавий инфратузилмани қўллаш муҳим аҳамиятга эга»[59] деб кўрсатилиши рақамли иқтисодиётни ривожлантириш инфратузилмасини амалга ошириш кўзда тутилган. Ўқув қўлланмани ўзлаштириш натижасида талаба: ¬ рақамли иқтисодиётнинг технологик, ҳолатий, ташкилий-ҳуқуқий ҳамда институционал ҳусусиятларини инобатга олган вазиятларни тўғри моделлаштириш, рақамли иқтисодиёт

[57] 3Мирзиёев Ш.М. Ўзбекистон Республикаси Президенти Ш.М.Мирзиёевнинг Олий Мажлисга Мурожаатномаси. // Халқ сўзи, 2022 йил.

[58] Ўзбекистон Республикасининг “Илм-фан ва илмий фаолият тўғрисида”ги Қонуни, 29 октябр 2019 йил.

[59] Ўзбекистон Республикаси Президентининг «Рақамли иқтисодиётни ривожлантириш мақсадида рақамли инфратузилмани янада модернизация қилиш чора-тадбирлари тўғрисида»ги Қарори// «Халқ сўзи» газетаси, 22 ноябрь 2018 йил

инфратузилмасини ташкил этиш; “блокчейн” технологияларнинг моҳиятини англаб етиш; глобал ахборот ресурс базаларидан самарали фойдаланиш усул ва йўлларини билади ва улардан фойдалана олади;

- рақамли иқтисодиётни ривожлантириш, “блокчейн” технологияларини жорий этиш; давлат хусусий шериклик шартларида рақамли иқтисодиётни ривожлантириш, крипто-биржалар фаолиятини ташкил этиш, энг истиқболли ва стратегик муҳим лойиҳаларни амалга ошириш кўникмаларига эга бўлади;
- рақамли трансформациясининг ижобий ҳамда салбий оқибатлари, уларга таъсир этувчи омилларни аниқлаш; рақамли иқтисодиётнинг макро ҳамда микро даражадаги кўрсаткичларга таъсирини баҳолаш; рақамли трансформация самарадорлигини баҳолаш;
- ахборот хавфсизлиги муаммоларини аниқлаш; давлат хусусий шерикчилик асосида рақамли иқтисодиётни ривожлантириш учун платформалар ташкил этиш кўникмаларига эга бўлади.

Юқоридагиларга асосланиб, Ўзбекистон Республикаси иқтисодиёт тармоқларида олиб борилаётган иқтисодий ислоҳотлар йўналишларининг мазмун ва моҳиятини ҳамда корхоналарда рақамли иқтисодиётни қўллашда Ўзбекистон Республикаси Олий Мажлиси томонидан қабул қилинган қонунларга, Ўзбекистон Республикаси Президенти Ш.М.Мирзиёев асарларига, Президент фармон ва қарорларига, Вазирлар Маҳкамасининг қарорларига асосланади. Бундан ташқари, корхоналарда рақамли иқтисодиёт муаммолари билан шуғулланувчи профессорўқитувчилар, талабалар, тадқиқотчилар, илмий изланувчилар, тадбиркорлар ҳамда бошқа иқтисодиёт тармоқлари ходимлари ҳам фойдаланишлари мумкин.

AYOLLAR O‘RTASIDA KIBERJINOYATLARNI OLDINI OLISH MASALALARI

Muhammadjonova Gulasal Muzaffar qizi

Namangan davlat universiteti Yuridik fakulteti 1-bosqich talabasi

Annotatsiya. Mazkur maqolada bugungi kunda eng dolzarb mavzulardan biri bo‘lgan ayollar jinoyatchiligi, kiberjinoyat, ularning turlari haqida so‘z boradi. Ayollar orasidagi jinoyatchilik salmog‘i, ya’ni statistikasi, ayollarning bu yo‘lga kirish sabablari hamda buni oldini olish va shu bilan bog‘liq masalalar tahlil qilinadi.

Kalit so‘zlar: ayol, jinoyat, ayollar jinoyatchiligi, kiberjinoyat, firibgarlik, kiberbullying, onlayn ta’qib, davlat siyosati, oila, o‘g‘rilik, maxfiy ma’lumotlar.

Ayol bu – buyuk xilqat, hayot davomiyligining sababchisi, jamiyatimizning poydevori. Ayolni e’zozlash, unga hurmat ko‘rsatish sharq xalqlarining madaniyatiga, shu jumladan, o‘zbek xalqiga xos bo‘lgan xususiyatlaridan biri hisoblanadi. Mamlakatimiz o‘z mustaqilligini qo‘lga kiritgandan so‘ng qabul qilingan bir qator qonunlarimizda ayollar huquqlari inson huquqining alohida ajralmas qismi sifatida e’tirof etila boshlandi. Shu sababli ham mamlakatimizning bugungi kun siyosiy

hayotida, davlat va jamiyat ishlarida, iqtisodiyotning barcha tarmoqlarida, madaniyat, ilm-fan, sog‘liqni saqlash, sport va shu kabi ijtimoiy sohalarda ayollarning roli va o‘rni ortib borayotganini ko‘rishimiz mumkin.Bundan tashqari, ayollarning huquq va erkinliklari Asosiy Qonunimiz bilan birga ko‘plab hujjatlarda mustahkamlanganligidan ayollar borasidagi masalalar davlat siyosati darajasida ko‘tarilganligini bilishimiz mumkin. Shunga qaramasdan, ayollar tomonidan huquqbuzarliklar sodir etilishi, ularning jinoyat ko‘chasiga kirib qolish holatlari barchamiz uchun achinarlidir.

Jamiyat va davlatning ertasi bevosita xalqning kelajagi bo‘lmish farzandlarni dunyoga keltirib, ularni tarbiya qilayotgan ayollarning qo‘lida ekanligi alohida ahamiyatga ega. Ammo mana shunday yosh avlod tarbiyasi bilan shug‘ullanayotgan ayollarning turli xil jinoyatlarga qo‘l urayotgani bugungi kun uchun yangilik emas. Bu esa jamiyat va davlat kelajak hayotining tahlika ostida qolayotganligidan darak beradi. Bundan tashqari, ayollar tomonidan sodir etilayotgan jinoyatlar erkaklarnikidan ko‘ra ko‘proq hissiy xususiyatlarga bog‘liq ekanligini ta’kidlashimiz lozim. Umuman olganda, statistik ma’lumotlar shuni ko‘rsatadiki, jinoyat sodir etganlarning umumiy sonida ayollarning ulushi taxminan 15.5%ni tashkil etadi. Shu bilan birga, jinoyatchi ayollarning yarmidan ko‘pi 30 va undan katta yoshdagi ayollar hisoblanadi. Bu ko‘rsatkich erkaklarnikiga nisbatan ancha past bo‘lishi mumkin, lekin ayollar tomonidan sodir etilayotgan jinoyatlarning ijtimoiy xavflilik darajasi anchayin yuqoriligi bilan ajralib turadi. 2021-yil ma’lumotlariga yuzlanadigan bo‘lsak, shu yil hisobotida jami jinoyatlarning 9.8%i ayollar ulushga to‘g‘ri kelgan.

Bu haqda: “Har doim ayollar jinoyati bilan bog‘liq statistika yuritib boriladi va ayollar tomonidan sodir qilinishi mumkin bo‘lgan jinoyatlarning oldini olish maqsadida profilaktika ishlari olib boriladi. Bugungi kunda jami jinoyatlarning 9,8 foizi ayollarga tegishli. Ammo, bu ham juda achinarli holat”, deydi Toshkent shahar sudi raisi o‘rinbosari – jinoyat ishlari bo‘yicha sudlov hay’ati raisi Akbarali Turobov.

Hozirgi kunda ayollar tomonidan sodir etilayotgan jinoyatlar tasnifiga e’tibor beradigan bo‘lsak, firibgarlik, talonchilik, o‘g‘rilik va shu kabi bir qancha jinoyatlarni keltirishimiz mumkin. Bunga qo‘shimcha sifatida hozirgi paytda butun dunyo aholisini qiynab kelayotgan global tusdagi jinoyatlardan biri kiberjinoyatni ham aytishimiz maqsadga muvofiqdir. Ushbu jinoyat ko‘pincha erkaklar tomonidan sodir etilishiga qaramasdan, jinoyatning sodir etilishida ayollarning ham ulushi ortib bormoqda. Ya’ni, kiberjinoyat erkaklar tomonidan ko‘proq amalga oshirilishi mumkin, chunki erkaklar ko‘proq texnik jihatdan kiberhujumlar, tizimlarni buzish, viruslarni tarqatish kabi faoliyatlarga jalb qilinadi. Biroq ayollar ham turli ko‘rinishdagi kiberjinoyatlarni sodir etishadi va bu jinoyat ham o‘ziga xos xususiyatlarga, sabablarga ega bo‘lishi mumkin.

Shu kunlarda ayollar orasida keng tarqalgan asosiy jinoyatlardan biri bu onlayn firibgarlikdir. Ya’ni hozirgi davrda turli xil maishiy buyumlar, tovarlar savdosi bilan shug‘ullanuvchi niqobida paydo bo‘layotgan soxta tadbirkor ayollarga duch kelayapmiz. Biror bir mahsulotni onlayn reklamasi orqali o‘zlari shaxsiy profil yuritib, mahsulot pulini o‘z hisobiga o‘tkazgandan so‘ng yo‘q bo‘lib qoladigan, odamlarning ishonchiga kirib ularni aldaydigan, firibgarlik yo‘li bilan mo‘maygina daromad orttirishni maqsad qilgan ayollar, afsuski, oramizda yo‘q emas. Bundan tashqari, ba’zi ayollar boshqalarni haqorat qilish, ularni ta’qib ostiga olish natijasida ruhiy va

psixologik zarar yetkazishadi. Ushbu jinoyat (kiberbullying) ijtimoiy tarmoqlarda keng tarqalgan jinoyatlardan yana biridir. Shaxsiy ma’lumotlarni o‘g‘irlash va foydalanish ham kiberjinoyat tarkibiga kirib, ayollar onlayn tizimlardan foydalanib, boshqa odamlarning shaxsiy ma’lumotlarini o‘g‘irlashlari va o‘z manfaatlari yo‘lida bundan foydalanishlari mumkin. Misol uchun, bank kartalarini o‘g‘irlash yoki identifikatsiya ma’lumotlarini ishlatib firibgarlik qilishlari mumkin.

Ayollar orasida kiberjinoyatlarning tarqalganlik statistikasiga kelsak, bu borada aniq ma’lumotlar juda cheklangan, chunki bu masalada ko‘plab tadqiqotlar va ma’lumotlar erkaklarning faoliyatiga ko‘proq qaratilgan. Ayollar ko‘proq kiberjinoyatlarning qurboni sifatida ko‘rilsa-da, ba’zi hollarda ayollar ham kiberjinoyatlarni sodir etishadi, ammo bu odatda erkaklarga nisbatan ayollar statistikasi kamroq uchraydi.

Kiberjinoyatning sodir etilish sabablari erkaklarda ham, ayollarda ham deyarli bir xil hisoblanadi.

Birinchidan, moliyaviy manfaatlar va foyda olish. Ayollar ba'zan moliyaviy foyda olish uchun kiberjinoyatlarni sodir etishadi. Masalan, soxta onlayn savdo, soxta investitsiya imkoniyatlari yoki maxfiy ma'lumotlarni o'g'irlash orqali pul topish va boshqalar. Internetda firibgarliklar va o'z manfaatlari uchun boshqalarni manipulyatsiya qilish kiberjinoyatlarning sodir etilishiga olib kelishi mumkin. Firibgarlik, odatda, boshqalarning ishonchini suiiste'mol qilish orqali amalga oshiriladi.

Ikkinchidan, onlayn ta’qib va boshqa hissiy sabablar ham ayollarni kiberjinoyat qilishga undashi mumkin. Masalan, ba’zi ayollar o‘zlarining raqiblari va boshqa maqsadli shaxslarga nisbatan haqorat qilish, ta’qib qilish, o‘zgalar oldida ularni yomon holatga solish orqali ham jinoyat sodir etilishi ehtimoldan holi emas.

Uchinchidan, o‘z manfaatlari uchun boshqalarning shaxsiy ma’lumotlarini o‘g‘irlash va ulardan noto‘g‘ri foyfalanish. Bu orqali esa boshqa odamlarni manipulyatsiya qilish maqsadi yotadi. Ammo bu jarayonlarning boshqa ko‘plab sabablari - bu insonning shaxsiy motivlari va ijtimoiy omillar bilan bog‘liq bo‘lishi ham mumkin.

Umuman olganda, kiberjinoyatlarning ham, boshqa jinoyatlarning ham sodir etilish salmog‘i ayollar orasida yuqorilashib bormoqda. 2021- yilda ishsiz ayollar o‘rtasida jinoyatchilik 1,7 baravarga, 18-30 yoshdagi xotin-qizlar tomonidan sodir etilgan jinoyatlar esa 2 baravarga ko‘paygan. Bu shundan dalolat beradiki, jinoyatlarning barchasining tag zamirida bekorchilik, ayollar bandligining ta’minlanmaganligi yotadi.

Sud amaliyotining ko‘rsatishicha, nojoiz qilmishlar, jumladan, jinoyatlar ildizi oiladagi muhitga borib taqaladi. Jinoyatlarni odob-axloq, ta’lim-tarbiya yo‘lga qo‘yilmagan xonadon a’zolari sodir etadi. Oilaviy axloq esa ta’lim, madaniyat va shu kabi omillarga bevosita bog‘liq.

Ayollar tomonidan sodir etilgan jinjoyatlar bilan bog‘liq bir qancha omillar mavjud bo‘lib, A.G. Zakirovaning fikriga ko‘ra, ayollar tomonidan sodir etiladigan jinoyatlar jinoyat motivi bilan farq qilib, birinchi navbatda rashk, o‘ch olish, hasadgo‘ylik, jabrlanuvchidan qutulishga harakat qilishda namoyon bo‘lishi bilan izohlanadi.

Ayollar jinoyatchiligini oldini olish masalalariga keladigan bo‘lsak, bunda zarur bo'lgan shart-sharoit jamiyat hayotidagi mavjud muammolarni bartaraf etish bilan yonma-yon amalga oshirilmog'i lozim. Aytish mumkinki, ayollar jinoyatchiligining oldini olish o'ziga xos g'oyaviy va ma'naviy ahamiyatga ham ega. Ayollarning ijtimoiy muhofazasini ta'minlash oilani ham ma'naviy, ham moddiy jihatdan sog'lomlashtirish va yangi avlodni tarbiyalashni talab darajasida bo'lishini ta'minlaydi. Ayollar jinoyat sodir etishining oldini olish uchun uning shakllanishiga salbiy ta'sir etuvchi omillarni aniqlash lozim. Bunday omillar esa asosan maishiy turmush va ishlab chiqarishda yuzaga keladi.

To'g'ri, jamiyatda ma'lum bir vazifaning bajarilishini ta'minlash uchun unga zarur muhit yaratish lozim. Shunday ekan, ayollar jinoyatlariga yo'l qo'ymaslik uchun ishlab chiqarish, dam olish, oilaviy yo'nalishlarda uchraydigan muammolarni yechish katta ahamiyatga ega. Ularni yechmay turib ayollar jinoyatchiligining oldini olishda ijobiy natijalarga erishib bo'lmaydi.
Ma'lumki, maishiy hayotda alohida e'tiborga molik muammo oilani har tomonlama ta'minlash. Aynan oilani mustahkamlash ayollar sodir etadigan juda ko'p jinoyatlarning oldini olishdagi birinchi qadamdir.

Gap oila to‘g‘risida borar ekan, aynan oilada qiz bolaning tarbiyasiga alohida e'tibor qaratish lozimligini e'tibordan chetda qoldirmaslik kerak. Qizlarni yoshlikdan odobli, iffatli qilib tarbiyalash, ayollik xususiyatlarini shakllantirishga erishish darkor. Zotan, erkaklarga xos sifatlarning qiz bola tomonidan egallanishi, ularda rahmsizlik bo'lishi, tasodifan ko'cha bolasiga aylanishi yoki ular safiga qo'shilib, shafqatsizlik kabi xislatlarning shakllanishiga olib keladi. Qiz bolalarning nazoratsiz, oiladan tashqarida qolishi xavfli bo‘lib, shu orqali jinoyat ko‘chasiga kirib qolishi ehtimoldan yiroqda emas.

FOYDALANILGAN ADABIYOTLAR

1.”Kiberxavfsizlik to‘g‘risida”gi Qonun 15.04.2022
2. “Davlat xavfsizlik xizmati to‘g‘risida”gi Qonun 25.06.2024
3. Qalampir.uz sayti
4. Daryo,uz sayti.

КИБЕРХАВФСИЗЛИКНИ ОЛИНИ ОЛИГА ДОИР АЙРИМ МУЛОҲАЗАЛАР

Шукуруллоев Шодиёр Тўражонзода

Наманган давлат университети Юридик факультети 3-босқич талабаси

Бугунги кунда жамиятимизда глобал муаммолари қаторига янгидан-янги турлари билан тилга олинаётган кибержиноятчилик кириб келганига ҳам анча бўлди. Унинг бизга маълум бўлган вирусли дастурларни тарқатиш, паролларни бузиб кириш, кредит карта ва бошқа банк реквизитларидаги маблағларни ўзлаштириш талон-торож қилиш, шунингдек, интернет орқали қонунга зид ахборотлар, хусусан, бўҳтон, маънавий бузуқ маълумотларни тарқатиш билан башарият ҳаётига катта хавф солаётганидан кўз юма олмаймиз.

Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан хар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.[1]

Ахборотнинг ҳимояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатьий регламентланган динамик технологик жараёнга айтилади.

Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан хар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.[2]

Ахборотнинг ҳимояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатьий регламентланган динамик технологик жараёнга айтилади.

Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан хар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.

Ахборотнинг ҳимояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатьий регламентланган динамик технологик жараёнга айтилади.

Киберхавфсизлик тушунчасига таърифлар мавжуд. Хусусан, CSEC2017 Joint Task Force (CSEC2017 JTF) киберхавфсизликка қуйидагича таъриф берган:

Киберхавфсизлик – ҳисоблашга асосланган билим соҳаси бўлиб, бузғунчилар мавжуд бўлган шароитда амалларни кафолатлаш учун ўзида технология, инсон, ахборот ва жараённи мужассамлаштирган. ¬ У хавфсиз компьютер тизимларини яратиш, амалга ошириш, таҳлил қилиш ва тестлашни ўз ичига олади.[3]

Киберхавфсизлик таълимнинг мужассамлашган билим соҳаси бўлиб, қонуний жихатларни, сиёсатни, инсон омилини, этика ва рискларни бошқаришни ўз ичига олади.

Тармоқ бўйича фаолият юритаётган Cisco ташкилоти эса киберхавфсизликка қуйидагича таъриф берган:

Киберхавфсизлик – тизимларни, тармоқларни ва дастурларни рақамли ҳужумлардан ҳимоялаш амалиёти. Ушбу киберҳужумлар одатда махфий ахборотни бошқариш, алмаштириш ёки йўқ қилишни; фойдаланувчилардан пул ундиришни; ёки нормал иш фаолиятини узуб қўйишни мақсад қилади.

Ҳозирги кунда самарали киберхавфсизлик чораларини амалга ошириш инсонларга қараганда қурилмалар сонининг кўплиги ва бузғунчилар салоҳиятини ортиши натижасида амалий томондан мураккаблашиб бормоқда.

Киберхавфсизлик концепцияси – ахборот хавфсизлиги муаммосига расмий қабул қилинган қарашлар тизими ва уни замонавий тенденцияларни ҳисобга олган ҳолда ечиш йўллари.

Киберхавфсизлик сиёсати бу – ташкилотнинг мақсади ва вазифаси ҳамда хавфсизликни таъминлаш соҳасидаги чора-тадбирлар тавсифланадиган юқори сатҳли режа ҳисобланади. У хавфсизликни таъминлашнинг барча дастурларини режалаштиради. Аппарат воситалар ва дастурий таъминот иш жараёнини таъминловчи воситалар ҳисобланади ва улар хавфсизлик сиёсати томонидан қамраб олиниши шарт.[4]

Ташкилотнинг амалий хавфсизлик сиёсати қўйидаги бўлимларни ўз ичига олиши мумкин: умумий низом; паролларни бошқариш сиёсати; фойдаланувчиларни идентификациялаш; фойдаланувчиларнинг ваколатлари; ташкилот ахборот коммуникацион тизимини компьютер вируслардан ҳимоялаш; тармоқ уланишларини ўрнатиш ва назоратлаш қоидалари; электрон почта тизими билан ишлаш бўйича хавфсизлик сиёсати қоидалари; ахборот коммуникацион тизимлар хавфсизлигини таъминлаш қоидалари; фойдаланувчиларнинг хавфсизлик сиёсатини қоидаларини бажариш бўйича мажбуриятлари ва ҳ.к.лар.

Ахборот хавфсизлиги сиёсати ташкилот масалаларини ечиш ҳимоясини ёки иш жараёни ҳимоясини таъминлаши шарт.

Бугунги кунда Ўзбекистон Республикасида “Киберхавфсизлик тўғрисида”ги қонун қабул қилинди. Қонуннинг мақсади мамлакатда киберхавфсизлик соҳасидаги муносабатларни тартибга солишдан иборат бўлиб, унинг асосий вазифалари кибермаконда шахс, жамият ва давлат манфаатларини ташқи ва ички таҳдидлардан ҳимоя қилиш ҳисобланади. Қонунда кибержиноятчилик, кибертаҳдид, киберхавфсизлик, киберҳимоя ва киберҳужум каби тушунчалар қўлланиб, киберхавфсизликни таъминлашнинг асосий принциплари ва бу соҳадаги давлат сиёсати асосий йўналишлари белгилаб берилган.[5]

Давлат хавфсизлик хизмати киберхавфсизлик соҳасидаги ваколатли давлат органи этиб белгиланиб, унинг ҳуқуқлари ва мажбуриятлари мустаҳкамлаб қўйилмоқда.

Қонун билан киберхавфсизлик субъектларининг ҳуқуқ ва мажбуриятлари, уларнинг киберхавфсизлик талабларига мувофиқлиги юзасидан экспертизадан мажбурий тартибда ёки киберхавфсизлик субъектлари ташаббусига кўра амалга оширилиши белгилаб қўйилди.

“Қонуннинг қабул қилиниши, биринчидан, шахс, жамият ва давлатнинг хавфсизлигини таъминлашда муҳим аҳамият касб этади;

иккинчидан, киберхавфсизликни давлат томонидан тартибга солиш, ҳуқуқий, ташкилий, илмий-техник ва меъёрий услубий таъминот тизимини такомиллаштиришга, ахборот тизимлари ва ресурсларининг яхлитлигини таъминлашга салмоқли ҳисса қўшади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 |Pages: 357
2. Эргашев А.А., Садикова Ф.С. Способы и методы анализа многомерного базы данных Universum: технические науки. Выпуск: 12(93) Декабрь 2021. С. 86-90
3. Imomova Shafoat Mahmudovna, Norova Fazilat Fayzulloyevna. Ta'lim jarayonlarini raqamli texnologiyalar asosida takomillashtirish// Miasto Przyszłości, Vol. 32 (2023), C.47-49.
4. Эргашев А.А., Умуров О.Ф. Выбор паттерна проектирования автоматизированной информационной системы Журнал Проблемы науки 2021 год июнь 6`65 . С. 17-19
5. Shafoat IMOMOVA. BLOCKCHAIN VA UNING AXBOROT XAVFSIZLIGIGA TA'SIRI//Pedagogik mahorat. Maxsus son(2021 yil, derkabr),2021, C.88-90.

KIBERJINOYATCHILIKKA QARSHI KURASHISH BO‘YICHA XALQARO TAJRIBA

Anvarjonov Ahmadbek Oybek o‘g‘li
Ilmiy rahbar: yu.f.d.(PhD) I.Atamirzayev

Namangan davlat universtiteti Yuridik fakulteti 1-bosqich talabasi

Annotatsiya. Ushbu maqolada kiberjinoyatchilikka qarshi xalqaro tajribalarga tayangan holda, ya'ni chet davlat tajribalari va usullarini qo‘llab ko‘rish bo‘yicha bir qator takliflar va g‘oyalar ilgari surilgan.

Kalit so‘zlar: kiberjinoyat, jinoyatchi, kibermakon, kiberxavfsizlik, internet, texnologiya, infrotuzilma

Hozirgi globallashuv davrida jahon internet axborotidan foydalanish, turli xil ma'lumotlar, hujjatlar va hattoki pul mablag‘larini boshqa bir joydan boshqa bir shaxsga o‘tkazish imkoniyati mavjud bo‘lib kelmoqda va takomillashmoqda. Biroq shu qatori fuqarolarning ushbu kommunikatsiya vositalaridan foydalanish usullari va shartlari bilan to‘liq tanish emasligi yoki tushunmasligi oqibatida internet tizimida ommalashgan kiberjinoyatchilar qurboni bo'lib qolishmoqda. Internet rivojlangani sari kiberjinoyatchilik ham avj olmoqda.

Kiberjinoyat - bu kompyuter texnologiyalari, internet yoki axborot tarmoqlaridan foydalangan holda kibermakonda amalga oshiriladigan jinoyatlar. Unda jinoyatchi axborot tizimlariga zarar yetkazish, shaxsga doir ma'lumotlarni o‘g‘irlash, firibgarlik yoki kompaniya va tashkilotlarning ma'lumotlariga zarar yetkazish va boshqa shu kabi maqsadlarni ko‘zlaydi.

Kibermakon- axborot texnologiyalari yordamida yaratilgan virtual muhit.

Kiberjinoyatlarning ham o‘z turlari mavjud bo‘lib ular har biri alohida usullardan foydalangan holda jinoyatni amalga oshirishni nazarda tutadi:

birinchisi: Xakerlik (hacking), bunda jinoyatchi biror bir davlat tashkiloti yoki kompaniya, shirkatlarning ma'lumotlarini uning xavfsizlik tizimini buzish orqali egallaydi

ikkinchisi: Fishing (phishing), bunda jinoyatchi internetda firibgarlik yo‘li bilan jabrlanuvchi shaxsning shaxsiy ma’lumotlarini qo‘lga kiritadi va boshqa jinoiy maqsadlarda shu ma’lumotlardan foydalanadi, natijada jabrlanuvchi o‘z o‘zidan jinoyatchi maqomiga ham ega chiqadi

uchinchisi: Zararli dasturlar tarqatish, bunda jinoyatchi turli xil virus, troyan va boshqa dasturlar orqali axborot tizimlariga zarar yetkazadi

to‘rtinchisi: Onlayn tovlamachilik (ransomware), bunda jinoyatchi ko‘pincha kriptovalyuta ya’ni raqamli valyuta turi bunda hisob kitoblar markazlashmagani sababli jinoyatchini aniqlash imkonsiz. Va bir qator shu kabi kiberhujum turlari mavjud.

Axborot quroli hujumda va mudofaada “electron tezlik” bilan ishlatilishi mumkin. Bu quroldan foydalanish axborot terrorizimidan himoyalanish maqsadida foydalaniladi, foydalanuvchilarga dunyo tarmoqlarida ishlashni ta’minlovchi mamlakatlarning milliy axborot resusrslarining zaifligi- har ikki tomonga zaif narsa.

Axborot quroli deganda axborot massivlarini yo‘qotish, buzish yoki o‘g‘irlash vositalari, himoyalash tizimini yo‘qotish, qonuniy foydalanuvchilar faoliyatini chegaralash asbob-uskunalar va butun kompyuter tizimi ishlashi tartibini buzish vositalari tushuniladi.

Hozirda hujumkor axborot quroli sifatida quyidagilarni ko‘rsatish mumkin: kompyuter viruslari, mantiqiy bombalar, telekommunikatsiya tarmoqlarida axborot almashinuvini bostirish vositalari, testli dasturlarni betaraflashtirish vositalari va boshqalar.

Ushbu jinoyatlarni oldini olishda kiberxavfsizlik bo‘yicha mutaxassislar yetishmasligi oqibatida butun dunyo kiberjinoyatlar og‘ushida qolgan. Statistic ma’lumitlarga qaraganda dunyo miqyosida 3 milliondan ortiq kiber mutaxassislar ehtiyoji mavjud bo‘lib buning 2 milliondan ziyodi bizning o‘kamizga ya’ni O‘rta osiyoga tegishli. Amerikada 300 ming, Yevropada 160 ming mutaxassis yetishmayabdi.

Ta’kidlanishicha O‘zbekistonda 2023-yilda 5,5 mingdan ziyod kiberjinoyatlar sodir etilgan. Shundan 70 foizi bank kartalari bilan bog‘liq firibgarlik va o‘g‘rilik jinoyatlari hisoblanadi.

Bunday jinoyatlarni oldini olishda bir qancha xalqaro darajadagi usullardan foydalanish mumkin. Misol uchun Fransiya davlatida kiberjinoyatlar avj ola boshladi va bunga “telegram” ijtimoiy tarmog‘i sabab bo‘ldi. Chunki bu tarmoqda barcha ma’lumotlar sir saqlanishi va hattokki asosli hujjatlarsiz davlat hukumatlariga ham oshkora qilinmaganligi sababli bu tarmoq kiberjinoyat sodir etish uchun jinoyatchilarga juda katta qo‘l keladi. Shu sababli Fransiya hukumati “telegram” ijtimoiy tarmog‘i asoschisi Pavel Durov bilan kelishishga urundi, ammo Pavel bunga boshida rozi bo‘lmaganligi sabab hukumat barcha jinoyatlarda uni ayblab hibsga olishiga sabab bo‘ldi. Biroz muddatdan so‘ng Pavel Durov bilan murosaga kelishildi va Fransiya hukumati “telegram” ijtimoiy tarmog‘ida shaxslarga doir ma’lumotlarga ega chiqishiga vakolat oldi.

Xalqaro tajriba sifatida Shimoliy Koreya siyosatini ham keltirish mumkin. Sababi bu davlatda axborot izlash, olish va tarqatish bilan bog‘liq cheklovlar mavjud. Ya’ni bu davlat fuqarolari internetdan foydalanishda tor vakolatga ega va

ma’lumotlarga qaraganda Shimoliy Koreyada maxsus o‘z internet tarmog‘i va ijtimoiy tarmoqlari mavjud. Shu sababdan bu davlat ko‘rsatkichida kiberjinoyatlar boshqa davlatlarga nisbatan past.

Amerika Qo‘shma Shtatlari ham dunyada eng rivojlangan xavfsizlik tizimiga ega. Sababi bu davlatda maxsus milliy infratuzilmalarni himoya qilishga mas’ul agentlik (CISA) faoliyat olib boradi.

Yevropa Ittifoqi ham umumyevropalik infratuzilmalar va shaxsiy ma’lumotlarni himoya qilish uchun integratsiyalangan siyosat yuritadi. Kiberxavfsizlik standartlarini ishlab chiqish va ularni rivojlantirish agentligi (ENISA) faoliyat ko‘rsatadi va NIS derektivasi (davlat va xususiy sektor o‘rtasidagi hamkorlikni oshirish uchun qabul qilingan qonun), (GDPR) fuqarolarning shaxsiy ma’lumotlarini himoya qilish bo‘yicha qat’iy qonunlar kuchga kirgan.

Xitoyning kibersuverenitet siyosati ham bu davlatga samarali foyda keltiradi. Bu davlatda internetga kirishni nazorat qilish va xorijiy veb-saytlarni cheklash (Great Firewall) tizimi mavjud.

Bunday tajribalardan aynan foydalanishning bir qator samarali va salbiy jihatlari mavjud. Samarali jihatla sarasiga natijani keltish mumkin ya’ni kiberjinoyatlar ko‘rsatkichi keskin tushishi hamda oldi olinishi. Salbiy jihati esa inson huquqlari cheklanishi va qulay imkoniyatlardan foydalanish imkoniyati pasayishi. Shimoliy Koreya siyosati o‘ziga xosligi bilan ajralib turadi, ammo u yerda inson huquqlari demokratlashmagan va erkinliklar ham yetarli darajada cheklangan.

O‘zbekiston Respublikasida ham kiberjinoyatlarni oldini olish bo‘yicha bir qartor ishlar amalga oshirilmoqda jumladan, prezidentimiz Shavkat Mirziyoyev 2022-yilda Shanxay Hamkorlik Tashkilotining Samarqandda bo‘lib o‘tgan sammitida kibermakondagi tahdidlarga qarshi nutq so‘zladi. Prezident bu nutqda internetdan noqonuniy maqsadlarda, jumladan, ekstremizm va terrorizmni targ‘ib qilishda foydalanilayotganiga alohida e’tibor qaratdi, bu tahdidlar nafaqat alohida mamlakatlar, balki butun mintaqa xavfsizligiga tahdid solishini ta’kidladi.

Shuningdek, O‘zbekiston Respublikasi Qonunchilik Palatasi tomonidan 2022-yil 25-fevralda qabul qilingan va Senat tomonidan 2022-yil 17-martda ma’qullangan maqsadi kiberxavfsizlik sohasidagi munosabatlarni tartibga solishdan iborat “Kiberxavfsizlik to‘g‘risida”gi O‘zbekiston Respublikasi qonuni qabul qilindi.

Ushbu qonunda kiberxavfsizlik sohasidagi yagona davlat siyosatini O‘zbekiston Respublikasi Prezidenti belgilaydi. O‘zbekiston Respublikasi Davlat xavfsizlik xizmati esa kiberxavfsizlik sohasidagi vakolatli davlat organi sifatida biriktirildi.

Ammo bu qonun samaraliroq ishlashi va natijasi ko‘rinishi uchun yuqorida ta’kidlanganidek kiber mutaxasisslar kerak. Bunday kadrlarni tayyorlash va malakasini oshirish bo‘yicha maxsus chora tadbirlar misol uchun, o‘quv darsliklar, tanlovlar, konferensiyalar, taqdimotlar, media sohasidagi rag‘batlantirishlar amalga oshirish, shuningdek, yuqoridagi davlatlar singari maxsus agentlik yoki tashkilotlar tashkil etish samarali foyda keltiradi.

Xulosa qilib shuni aytish mumkinki, kiberxavfsizlik va axborot xavfsizligini ta’minlash uchun xalqaro tajribalarga tayanish asosli bo‘ladi va O‘zbekiston Respublikasi siyosatida ham bir qancha qulaylilklar yaratiladi.

FOYDALANILGAN ADABIYOTLAR

1. “Kiberxavfsizlik to‘g‘risida”gi O‘zbekiston Respublikasi qonuni 2022- yil
2. G‘aniyev S.K., Karimov M.M., Tashev K.A. “AXBOROT XAVFSIZLIGI” Toshkent nashriyoti 2007-yil
3. Kun.uz rasmiy veb sahifasi
4. Gazeta.uz rasmiy veb sahifasi

KIBER JINOYATCHILIKGA QARSHI KURASH *(XALQARO TAJRIBA)*

Abdulaxadov Bekmuhammad Avazbek o‘g‘li

Namangan davlat universiteti Yurisprudensiya yo‘nalishi 1- bosqich talabasi

Annotatsiya. Ushbu maqolada kiberjinoyatlarga qarshi kurashish to‘g‘risida xalqaro tajribaga tayangan holda yoritilgan (ma’lumot berilgan) va bunday huquqbuzarliklar oqibatida qanday jinoyatlar sodir etilishi aytib o‘tilgan hamda bu kabi illatlar mamlakatlar taraqqiyotiga ta’sir ko‘rsatadigan salbiy tomonlari yoritilgan.

Kalit so‘zlar: kiberjinoyat, kibertovlamachilik, kiberxavfsizlik, kiberterrorizm, kiberhujum, dark net, inert pol, yeuro pol.

Bugungi kunda kiber jinoyatlar ko‘plab xorijiy davlatlarda xususan O‘zbekistonda ham ko‘plab sohalarga asosan iqtisodiy hamda siyosiy sohalarga katta havf solmoqda. Hozirgi kommunikatsion axborot texnologiyalari zamonida ham afsuski bu kabi vertual (kiber) jinoyatlar oldida insoniyat ojiz qolmoqda, va bunga asosiy sabab esa fuqarolarning bu kabi kiber xavfsizlik to‘g‘risida yetarli darajada ma’lumotga ega emasliklari.

Shuningdek ko‘plab kiberjinoyatlarning ijtimoiy tarmoqlarda kuzatilmoqda. Hozirgi kunda barcha fuqarolar ijtimoiy tarmoqlardan nafaqat kundalik muloqot uchun balki o‘z shaxsiy ma’lumotlarini saqlash uchun ham foydalanmoqdalar, misol uchun:o‘z shaxsiga oid ma’lumotlar, telefon raqami, shaxsiy elektron manzili, yashash manzili qayerda ishlash yoki o‘qishi, ayniqsa elektron bank kartarimizdagi mablag‘larimiz xavf ostida qolishi mumkin.

Bu kabi jinoyatlarga yana bir qancha misollar keltirib turli hil sotsial tarmoqlardagi firibgarlar boshqa shaxslarning shaxsiy akkauntlariga ularning elektron ma’lumotlarni olgan holda kirib ularning hisoblaridan mablag‘larini yechib olishlari yokida shu shaxslarni o‘zini ham aldash firibgarlik yo‘li bilan bunday kiber jinoyatlarga yo‘naltirishlari mumkin. Jumladan qisqa muddat ichida katta mablag‘ni qo‘lga kiritishingiz mumkin yoki sizni tabriklaymiz siz qanchadir million summada mablag‘ yutib olishingiz mumkin degan kabi aldo‘v so‘zlar orqali boshqa fuqarolarni shunday jinoyatlarga aralashib qolishlariga hamda jabrlanivshlariga ham sabab bo‘lmoqda.

Kiberjinoyat - Kompyuter, Smartfonlar va internet tarmoqlari bilan birgalikdagi aloqasi orqali ulangan holda sodir etiluvchi jinoyat (huquqbuzarlik) hisoblanadi. Hozirgi XXI-asr axborot texnologiyalari davrida bu kabi kiberjinoyatlarning glaballashgan turi moliyaviy o‘g‘irlik, kiber tovlamachilik kabi turlari ommalashgan.Ushbu atamaga kiber terrorizm kabi atamalar ham bog‘liq bo‘lishi

mumkin, chunki bu kabi jinoyatlar nafaqat iqtisodiy tomondan balki turli hil davlat to‘ntarishlarida, davlat tuzumiga qarshi jinoyatlar kabi turlari ham kiritish mumkin.

Shuningdek bunday kiberjinoyatlarga qarshi kurashish uchun turli hil qonunlar chiqarilgan, bularga misol qilib: Amerika qo‘shma shtatlarida "Computer Fraud and Abuse Act" (CFAA) kabi qonunlar orqali kiberjinoyatlarga qarshi kurashiladi. Federal qidiruv byurosi (FBI) maxsus kiberjinoyatlar bo‘limiga ega.

Yevropa Ittifoqi davlatlarida General Data Protection Regulation (GDPR) orqali ma'lumotlar xavfsizligi va foydalanuvchilarning maxfiyligini ta'minlashga katta e'tibor qaratadi.

Dunyoning rivojlangan mamlakatlaridan biri Xitoy Kiberxavfsizlik bo‘yicha qat'iy qonunlarni joriy qilib, axborot nazoratini kuchaytirgan va shu kabi vertual jinoyatlarga qarshi samarali kurash olib bormoqda.

Bu kabi hujjatlardan tashqari bir qancha xalqaro tashkilotlar ham mavjud bo‘lib bularga — INTERPOL va EUROPOL xalqaro tashkilotlari kiradi: Ushbu xalqaro tashkilotlar davlatlar o‘rtasida axborot almashinuvi va qo‘shma operatsiyalarni tashkil etadi.

Masalan, INTERPOL'ning Cyber Fusion Centre markazi global kiberjinoyatchilarni kuzatib boradi va sodir etilishini oldini oladi.

Kiberjinoyatlar to‘g‘risida dunyoning shu sohaga yaqin bo‘lgan ko‘plab olimlar, xususan: Edward Snowden (Sobiq razvedka xodimi va axborot xavfsizligi bo‘yicha tanqidchi) hamda Marc Goodman (Kiberjinoyatchilik bo‘yicha ekspert va "Future Crimes" kitobi muallifi) o‘z fikrlarini bildirib o‘tishgan misol uchun Edward Snowden bu kabi jinoyatlarga shunday ta’rif bergan "Kiberjinoyatlar va xakerlik faqat jinoyatchilar emas, balki hukumatlar tomonidan ham sodir etiladi. Shuning uchun texnologiyalarni qanday boshqarayotganimiz muhim"[1] deb o‘z fikrini bildirib o‘tgan.

Bundan tashqari Marc Goodman ham o‘z fikrini bildirib o‘tgan, unga ko‘ra "Kiberjinoyatlar zamonaviy jinoyatchilikning yangi chegarasidir. Kelajakda jinoyatchilar sun’iy intellekt va robototexnikani ham o‘z maqsadlariga foydalanishlari mumkin."[2]

Shu kabi fikr mulohazalar bilan bu kabi olimlar turli hil kiberhujum va jinoyatlarga o‘z tarif va fikrlarini berib o‘tishgan

Kiberjinoyat turlari:

Moliya va firibgarlik bilan bog‘liq jinoyatlar — kredit karta firibgarligi

Identifikatsiya va shaxsiy ma’lumotlarini o‘g‘irlash — boshqa shaxslarning ma’lumotlarini o‘g‘irlash va shu ma’lumotlar orqali noqonuniy faoliyat ko‘rsatish va jabrlanuvchi shaxslar nomidan turli huquqbuzarliklar sodir etish

Xakerlik — Unauthorized access: dasturlar va tarmoqlarga ruxsatsiz kirish. Daniel of Service (DoS) va Distibuted Denial of Service (DDoS).

Kiberterrorizm va siyosiy jinoyatlar: Critical infrastructure attacks — Elektr stansiyalari transport tizimlari yoki davlat idoralariga hujumlar. Propaganda va dezinformatsiya— siyosiy maqsadlarda axborotlarni soxtalashtirish davlat siyosatiga bog‘liq ma’lumotlarni o‘g‘irlash, sotish o‘g’irlash.

Intelektual mulk huquqlarini buzish: mualliflik huquqiga ega asarlarni kitoblarni filmlarni va boshqa ahborotlarni ruxsatsiz tarqatish va o‘zlashtirish

Kiberjosuliklar: turli hil yirik kompaniyalardan ma’lumotlarni o‘g‘irlash hamda davlat organlaring tizimlariga kirib strategik va siyosiy ma’lumotlarni og‘irlash.

Shuni ham qo‘shimcha qilish kerakki hozirgi kunda ko‘plab rivojlangan davlatlarda kiberjinoyatchilar o‘z maqsadlarini amalga oshirishda "DARK NET" dan bir qancha ma’lumot va manbalar oladilar.

Darknet (yoki "Qorong'u tarmoq") internetning yashirin qismi bo‘lib, u an’anaviy brauzerlar orqali kirib bo‘lmaydigan maxsus tarmoqlarni o‘z ichiga oladi. Darknet Tor (The Onion Router), I2P (Invisible Internet Project) yoki Freenet kabi maxsus dasturlar yoki protokollar orqali ishlaydi. Bu tarmoq foydalanuvchilar uchun anonimlikni va maxfiylikni ta'minlashni maqsad qiladi.

Internetning bu yashirin va xavfliy bo‘lgan qismida jamiyki jinoyatlarni amalga oshirsa bo‘ladi:

- ✓ Narkotik moddalar, qurol-yarog‘ va soxta hujjatlar savdosi.
- ✓ Kredit karta ma’lumotlari va shaxsiy ma’lumotlarni o‘g‘irlash yoki sotish.
- ✓ Hacktivizm (xakerlik orqali siyosiy maqsadlarni amalga oshirish).
- ✓ Inson tanasi azolari savdosi (Odam savdosi).
- ✓ Yollanma xakerlik xizmatlari.

Shuningdek Dark Netda bzo bilgan xalqaro valyutalar: AQSH Dollari yokida Euro da sovdo qilishni iloji yo‘q bu tarmoqda kripta valyuta xususan bit coinda savdo qilinadi.

Hozirgi kundagi statistik ma’lumotlarga ko‘ra 2022 yilda Toshkentliklar kiberjinoyatlardan 45,2 milliard so‘m zarar ko‘rdi.

Bir yilda qayd etilgan jami jinoyatdan 3372 ta yoki 82 foizi bank plastik kartalardan pul mablag‘larni talon-toroj qilish bilan bog‘liq.

Moskvada (Rossiya, 12,6 mln aholi yashaydi) axborot texnologiyalari sohasida 105 360 ta kiberjinoyat qayd etilgan (2021 yilda — 103 600 ta, 2020 yilda — 102 060 ta kiberjinoyat);

Ostonada (Qozog‘iston, 1,3 mln aholi) bunday jinoyatlar 4822 ta aniqlangan (2021 yilda — 4224 ta, 2020 yilda — 5807 ta);

Minskda esa (Belarus, 2 mln ga yaqin aholi) 4773 ta kiberjinoyat sodir bo‘lgani haqida aniq ma’lumotlar bor. (2021 yilda — 4761 ta, 2020 yilda-4 773 ta);

Seulda (Janubiy Koreya, 10,5 mln aholi) 2022 yil 60450 ta kiberjinoyat aniqlangan (2021 yilda — 56210 ta, 2020 yilda — 60450 ta).

Bugungi kunda yurtimizda bu turdagi kiberjinoyatlarga qarshi kurashish uchun ko‘plab islohotlar olib borilmoqda, lekin birinchi o‘rinda fuqarolarning bu sohadagi aqliy-ijtimoiy salohiyatini oshirish maqsadga muvofiq bo‘ladi, chunki bu kabi jinoyatlar sodir etilishining asosiy omili fuqarolarning bu sohaga oid ma’lumotlarini bilmaganligi tufayli aldnishlari sabab bo‘lib kelmoqda. Va yana eng muhim omillardan biri fuqarolar o‘z shaxsiy ma’lumotlarini ijtimoiy tarmoqlarda saqlashni to‘xtatish lozim bilamizki barcha kiberhujum va shu kabi jinoyatlar ijtimoiy tarmoq platformalarida sodir etiladi.

Shuningdek bu kabi jinoyatlar uchun kuchli huquqiy choralar (sanksiyalar) o‘rnatilishi lozim bu yo‘l orqali kiberjinoyatlar soni kamayishi ehtimoli yuqori, misol uchun kibertovlamachilklar orqali boshqa shaxslarning elektron bank kartalaridan

mablag‘larini o‘zlashtirish uchun o‘rtacha 10-15 yil qamoq jazosi tayinlansa va yana shunga o‘xshash og‘ir jazolar tayinlasa kiberjinoyatlarning soni kamayishi mumkin bo‘ladi.

Bir so‘z bilan aytganda huquqiy chora tadbirlarni yanada takomillashtirish lozim: kiberjinoyatlarni aniqlash, jazo choralarini kuchaytirish, kiberjinoyatchilikga bog‘liq qo‘shimcha qonunlar qabul qilish, bu kabi jinoyatlarga qarshi turli hil xalqaro tashkilotlarga a’zo bo‘lish kerak.

Shuni ham qo‘shimcha qilish kerakki bu islohotlarni nafaqat davlatning ichkarisida balki tashqi siyosatda, xalqaro tashkilotlarda ham mustahkamlab yanada takomillashtirish lozim va davlatlararo kiberxavfsizlik standartlarini ishlab chiqish va ularga rioya qilish. Shu kabi islohotlar va taraqqiyotlar orqali kiberjinoyat kabi illatlarni oldini olishimiz va yo‘q qilishimiz mumkin.

Innovatsion rivojlanish, axborot siyosati va axborot texnologiyalari masalalari qo‘mitasi ushbu qonun loyihasini O‘zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasining majlisida birinchi o‘qishda ko‘rib chiqish uchun tayyorlandi.[3]

O‘zbekiston Respublikasining Kiberxavfsizlik to‘g‘risidagi qonunining 4 - moddasida kiberxavfsizlikni ta’minlashning asosiy prinsiplari sanab o‘tilgan:

- ❖ qonuniylik;
- ❖ kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi;
- ❖ kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv; kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;
- ❖ O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi,[4] shu kabi prinsiplari keltirib o‘tilgan.

Xulosa qilishimiz mumkunki, Kiberjinoyatlar bugungi kunda dolzarb muammoga aylangan va har bir yo‘nalish-sohalarga zarar keltirayotgan illatlardan biri hisoblansada unga qarshi mazkur qonun va qonun osti xujjatlarda belgilangan vazifalarni tizimli ravishda amalga oshirilsa. Bu salbbiy illatga qarshi kurash o‘z samarasini beradi.

FOYDALANILGAN ADABIYOTLAR

1. O‘zbekiston Respublikasi Kiberxavfsizlik to‘g‘risidagi QL-1134 sonli qonuni, Toshkent, 11.03.2024.
2.Edward Snowden (Sobiq razvedka xodimi va axborot xavfsizligi bo‘yicha tanqidchi)
3. Marc Goodman kiberjinoyatchilik bo‘yicha ekspert va "Future Crimes" AQSH, 02.24.2015
4.O‘zbekiston Respublikasi Kiberxavfsizlik to‘g‘risidagi qonunning 4 - moddasi Toshkent . 17.07.2022.

YANGI O‘ZBEKISTON SHAROITIDA KIBERJINOYATLARNING SODIR ETILISHIDAGI MUAMMOLAR

Jumaboyev Mirafzal Bahromjonov o‘g‘li

Namangan davlat universtiteti Yuridik fakulteti 1-bosqich talabasi

Annotatsiya. Ushbu maqolada kiberjinoyat tushunchasi va buning turli hil oqibatlari,kiberjinoyatning davlat va jamiyatga qanday salbiy ta’sir ko‘rsatishi,bu jinoyatni amalga oshirganlik uchun qonunda qanday jazo turlari borligi va buning oldini olish chora-tadbirlari yoritilgan.Tadqiqotda analiz va qiyosiy-huquqiy tahlil kabi metodlar qo‘llanilgan.

Kalit so‘zlar: kiber, kiberjinoyat, davlat, jamiyat, konvensiya, konstitutsiya, jinoyat.

Hozirgi davrda hayotimizni zamonaviy gadjetlarsiz tasavvur qilish qiyin. Albatta har bir sohada biz bevosiya mushkulimizni yengil qilish maqsadida bu zamonaviy texnologiya va ijtimoiy tarmoqlardan foydalanib kelmoqdamiz. Bu, albatta, biz uchun bir qancha qulayliklar tug‘diradi. Ammo, tanganing ikki tomoni bo‘lgani bois,bu sohada ham bevosita qing‘ir yo‘llar bilan pul topayotganlar ham yo‘q emas.

Misol uchun, ba’zi bir ijtimoiy tarmoqlarda yengil pul topish yo‘llarini ahtarib egri yo‘llarga kirib qolib bu qilmishlari uchun og‘ir badal to‘layotgan shaxslar ham yo‘q emas.Bu va bunday hodisalar bugungi kunda kundalik hayotimizda qulog‘imizga tez-tez chalinib turadi. Bu jinoyat zamonaviy qilib aytganda “Kiberjinoyat” deb nomlanadi.

Masalaning dolzarbligi shu yerda ko‘rinadiki, ko‘pgina odamlar bu shaxslarning qarmog‘iga oson o‘lja sifatida tushib qolmoqda.

Hodisani kengroq yoritish maqsadida avvalambor bu so‘zning asil ma’nosini tushunib olishimiz kerak bo‘ladi.

“Kiber” so‘zi, asosan, texnologiya va internet bilan bog‘liq bo‘lgan tushunchalarni ifodalash uchun ishlatiladi. Bu so‘z yunoncha “kybernetes” (boshqaruvchi yoki navigatsiya qiluvchi) so‘zidan kelib chiqqan.

Bu termin haqida bazi olimlar ham o‘z asarlarida shaxsiy fikrlarini bildirishgan.

Misol uchun, Dorothy Dening, Donn Parker ham ilmiy izlanishlarida bu illatga ta’rif berib kiberjinoyatchilikning oldini olish bo‘yicha muhim strategiyani ishlab chiqib ommaga taqdim qilib, kompyuter jinoyatlarini tasniflash va ularga qarshi kurashish usullarini ishlab chiqqan.[1]

Demak, kiberjinoyat ham bevosiya texnologiyalarga qaratilgan hujum ekanligini tushunib olish qiyin emas. Bu albatta,hozirgi yangilanayotgan O‘zbekistonning ko‘pgina iqtisodiy, ijtimoiy va albatta manaviy sohalariga o‘zining salbiy ta’sirini o‘tkazmay qolmaydi.

Har bir jinoyat turida bo‘lgani kabi bu jinoyatning ham bir qancha turlari mavjud:

Xakerlik - bu kompyuter tarmoqlari va shaxsiy sahifalarga ruxsatsiz kirish orqali jinoyat sodir etish xolati sanaladi.

Fishing - bu jinoyat tushunchasiga e’tibor bersak bunda sohta habarlar yoki reklamalar orqali odamlarni aldash orqali jinoyat sodir etish tushuniladi.

Identity theft (shaxsni o‘g‘irlash) - odamlarning ma’lumotlarini so‘roqsiz olish va ulardan noqonuniy foydalanish.

Kiberjinoyatlarning yana bir turi sifatida moliyaviy kiberjinoyatlarni keltirish mumkin. Bunday jinoyatlar turiga bank firibgarligi - banklarga qarshi moliyaviy jihatdan zarba berish va bank pullarini noqonuniy o‘zlashtirib olish kabi jinoyatlarni keltirish mumkin.

Kredit karta firibgarligi-kredit kartaning raqamini o‘zlashtirib,shaxsning shaxsiy pul mablag‘larini o‘zlashtirish jinyaoti va shular jumlasidandir.

Kripto valyuta firibgarligi - kriptovalyutalar, masalan, Bitcoin, Ethereum yoki boshqa raqamli aktivlardan foydalangan holda amalga oshiriladigan noqonuniy va aldovga asoslangan faoliyat xam bugungi kunda soni ortib boryotgan jinoyatlar turkumiga kiradi.

Ransomware bu jinoyat turi kompyuter yoki qurulmani bloklab qo‘yib,buning evaziga pul mablag‘ini undirilishini oz ichuga oladi

Botnetlar bu turli xil zararli botlar yaratib,ulardan g‘arazli yo‘llar uchun foydalanish tushuniladi.

DDoS hujumlari bu tarmoq yoki serverning faoliyatini buzish uchun ko‘plab qurilmalardan bir vaqtning o‘zida ortiqcha so‘rovlar yuboriladigan kiberhujum turi sanaladi

Tarmoqdan noqonuniy foydalanish bu ijtimoiy tarmoqdan qonunda man etilgan holda foydalanish tushuniladi

Yuqloridagi jinoyatlarning inson omiliga xosligi bilan axloqiy jinoyatlarni ham kiritish mumkin.

Yoshlar ahloqiga judda katta xavf soluvchi bola pornografiyasi - bolalar orqali sodir etilgan jinsiy tajovuzlar aks etgan rasm yoki videoroliklarni internet orqali tarqatish, onlayn ta’qib va taqdid-biror bir shaxsning shaxsiy sirlaridan foydalanib pul talab qilish kabi jinoiy arkatlardir.

Kiberbulling –i nternet yoki boshqa raqamli platformalar orqali bir kishiga nisbatan qasddan amalga oshiriladigan tahqirlash, haqoratlash, tahdid qilish yoki zo‘ravonlik harakatidir.

Bu jinoyatlarning barcha turi birinchi navbatda iqtisodiy va albatta, ijtimoiy jihatdan fuqarolarning huquq va erkinliklariga katta putur yetkazadi. Bundan kelib chiqadigan zararni hisoblashning esa imkoni yo‘q.Negaki,bu jinoyatlarning turlari texnologiya va ijtimoiy tarmoqlar rivojlangani sari kundan kunga ko‘payib,keng ildiz otmoqda.

Kiberjinoyat ko‘pgina davlatlarga, shu jumladan, O‘zbekiston Respublikasi va boshqa ko‘pgina dunyoning rivojlangan davlatlarga ham o‘z ta’sirini o‘tkazioqda.

Ko‘p hollarda kiberhujum harbiy, sog‘liqni saqlash va boshqa muhim sohalarga qaratiladi.

O‘zbekiston Respublikasida 2024 yilning 11 oy ichida 5500 tadan ortiq kiberjinoyat sodir etilgan.

AQSh esa 2024 yilning 2-yarmida 1692 marta kiberhujum qurboni bo‘lgan.

Yoki Xitoy Xalq Respublikasi va Hindistonni oladiga bo‘lsak, bu yil qariyb 500 milliondan ortiq kiberhujumlar qayd etildi. Bu o‘tgan yilning shu davriga niabatan 46

foizga oshgan. Statistik ma’lumotlar ko‘rsatib turibdiki,bu ko‘rsatkichlar yildan yilga oshib bormoqda.

Eng yaxshi himoya hujum deganlaridek, bu illatga qarshi dunyo hamjamiyati ham ko‘pgina chora-tadbirlarni ishlab chiqmoqda.

Hususan, 2024-yilda Birlashgan Millatlar Tashkiloti tomonidan Kiberjinoyatlarning oldini olish bo‘yicha konvensiya qabul qilindi. Bu konvensiya o‘zida quyidagi asosiy yo‘nalishlarni qamrab olgan:

1.Xalqaro hamkorlikni kuchaytirish.

2.Inson huquqlarini himoya qilish.

3.Kiberjinoyatlarni aniq belgilash.

Bu sohada mamlakatimizda ham ko‘pgina samarali chora-tadbirlar ko‘rib chiqilmoqda. Jumladan, Davlatimiz rahbari Shavlat Mirziyoyev boshchiligida kiberhavfsizlik sohasidagi qonunchilikni takomillashtirish maqsadida bir necha qonun hujjatlariga o‘zgartirishlar kiritildi. Bu o‘zgarishlar davlat axborot tizimlari va resurslarini himoya qilish,kiberhavfsizlik talablarini oshirishga qaratilgan edi.

Yuqorida ta’kidlanganidek, bu jinoyat turi mamlakat iqtisodiyoti va fuqarolarning huquqlariga jiddiy zarar yetkazmoqda va albatta bu huquqiy oqibat tug‘dirmay qolmaydi.

Mashhur olim Mark Goodman o‘zinimg asarida shunday deydi:”Jinoyatchilar har doim texnologiyalardan tezroq qiladi, ular doim yangi imkoniyatlarni tezroq anglab ulardan tezroq foydalanishga harakat qiladi”[3].

Bu shuni anglatadiki, kiberjinoyatchilar texnologiyalar bilan ishlagani bois yangilanishlarga tezgina moslashib ketishadi.

O‘zbekiston Respublikasi qonunchiligida kiberjinoyatning og‘ir oqibatlariga qarshi qo‘llaniladigan bir qancha sanksiyalar mavjud.

Misol uchun, O‘zbekiston Respublikasi Konstitutsiyasining 31-moddasida shunday deyilgan: “Har kim yozishmalari, telefon orqali so‘zlashuvlari, pochta, elektron va boshqa xabarlari sir saqlanishi huquqiga ega.

Ushbu huquqning cheklanishiga faqat qonunga muvofiq va sudning qaroriga asosan yo‘l qo‘yiladi. Har kim o‘z shaxsiga doir ma’lumotlarning himoya qilinishi huquqiga, shuningdek noto‘g‘ri ma’lumotlarning tuzatilishini, o‘zi to‘g‘risida qonunga xilof yo‘l bilan to‘plangan yoki huquqiy asoslarga ega bo‘lmay qolgan ma’lumotlarning yo‘q qilinishini talab qilish huquqiga ega” Yoki Jinoyat kodeksining 6-bo‘lim 10^1 bobida Kiberjinoyatlarga qarshi jazo choralari berilgan.

Misol uchun, 278-moddada Axborotlashtirish qoidalarini buzish, ya’ni belgilangan himoya choralarini ko‘rmagan holda axborot tizimlari, ma’lumotlar bazalari va banklarini, axborotga ishlov berish hamda uni uzatish tizimlarini yaratish, joriy etish va ulardan foydalanish hamda axborot tizimlaridan ruxsat bilan foydalanish fuqarolarning huquqlariga yoki qonun bilan qo‘riqlanadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga ko‘p miqdorda zarar yoxud jiddiy ziyon yetkazilishiga sabab bo‘lsa,-Bazaviy hisoblash miqdorining ellik baravarigacha miqdorda jarima yoki bir yilgacha axloq tuzatish ishlari bilan jazolanadi.

O‘sha harakatlar juda ko‘p miqdorda zarar yetkazgan holda sodir etilgan bo‘lsa, Bazaviy hisoblash miqdorining ellik baravaridan yuz baravarigacha miqdorda jarima yoki bir yildan ikki yilgacha axloq tuzatish ishlari bilan jazolanadi.

Avvalambor, biz kiberjinoyatning qurboniga aylanishimizga sabab bizning huquqiy ongimizda hali ham ba’zi oqsoqliklar borligi sabab bo‘lishi mumkin.Yoki, yoshlarning bo‘sh vaqtini mazmunli tashkil etilishi jihatidan oqsoqlanish sabab bo‘lishi mumkin.

Bunga yechim sifatida, fuqarolarning huquqiy va zamonaviy salohiyatini oshirish maqsadida turli hil jamoaviy tuzilmalar tashkil qilish, maktab, kollej va OTMlarda kiberjinoyatlarning kelib chiqish sababi, oqibati va uning oldini olish chora-tadbirlari haqida yanada ko‘proq tushuncha berish,yoshlarning bo‘sh vaqtini samarali va mazmunli tashkil etish uchun ularning qiziqishlariga mos bo‘lgan ilmiy va sport to‘garaklarida ishtirok etish uchun yetarli shart-sharoitlar yaratilishi zaruz.

Shuningdek bu jinoyatning og‘ir oqibatlari haqida tushuntirilishi kerak.Va yana, hech kimga sir emaski kiberjinoyatlarning asosiy qurbonlari yoshi katta fuqarolardir. Negaki ularning zamonaviy texnologiyalar bilan foydalanish ko‘rsatkichi yoshlarga qaraganda biroz pastroq.

Bundan kelib chiqadiki, ular yoshlarga nisbatan ko‘proq buning qurboni bo‘lishadi. Shuning uchun bunday fuqarolar uchun ham maxsus o‘quv-amaliy jarayonlarni tashkil etish kerak. Yoki, ommaviy axborot vositalarida, masalan, televideniye, gazeta va jurnallar, radio va ijtimoiy tarmoqlardagi ishonchli kanallar orqali ularga bu haqida uzluksiz ma’lumot berib borilishi kerak.

Kiberjinoyat yo‘liga kirib,jazoni o‘tab chiqqan fuqarolar uchun ham maxsus chora tadbirlar yanada ko‘proq yaratilsan mahsadga muvofiq bo‘ladi. Eng avvalo ularning bandligi ta’minlanishi kerak. Ularning bu boshi berk ko‘chaga boshqa qadam bosmasliglari kerakligi tushuntirilishi zarur va shart.

Ularning tezda yangi hayot boshlashi uchun davlat ularga yanada ko‘proq g‘amxo‘rlik qilishi kerak. Bu ularning kelgusidagi faoliyati uchun judda katta yordam bo‘ladi desak,adashmagan bo‘lamiz

Yuqoridagilardan xulosa sifatida kiberjinoyat mamlakatimiz va xalqimiz uchun qanchalik havf tug‘dirishini ko‘rib chiqdik. Bu birinchi navbatda mamlakat iqtisodiyotining darz ketishiga sabab bo‘ladi va albatta,buning tasiri fuqarolarga sezilmay qolmaydi. Bugungi kunda O‘zbekiston Respublikasining ko‘pgina qonun hujjatlari, jumladan, Jinoyat va Ma’muriy javobgarlik to‘g‘risidagi kodekslarga ham tez-tez o‘zgarish kiritilishining ham sabablaridan biri manashunday kelajak jinoyatlarining keng tatqalib borishidir.

Shunday ekan, biz ham o‘zimizning shaxsiy ma’lumotlarimizni sir saqlashimiz,do‘st tanlashda adashmasligimiz, har kuni zamonaviy texnologiyalar bilan yaqindan tanishib turishimiz kerak. Va albatta o‘zimizning huquqiy ong va huquqiy madaniyatimizni yanada oshirish maqsadida ko‘proq mutolaa bilan mashg‘ul bo‘lishimiz kerak.

Shu va shu kabi jinoyatlar guvohi bo‘ladigan bo‘lsak zudlik bilan tegishli organga murojat qilishimiz zarur. Shuni unutmasligimiz lozimki, kiberjinoyat birinchi o‘rinda davlatning iqtisodiyotiga katta zarar yetkazadi.

Bugun jamiyatimizda mazkur illatga qarshi barchamiz bir yoqadan bosh chiqarishimiz kerak.

Prezidentimiz Shavkat Mirziyoyev birlik to‘g‘risida shunday fikr bildirganlar:”Yurtimizning tinchligi va taraqqiyoti har bir fuqaroning birdamligi, bir

maqsad yo‘lida harakat qilishiga bog‘liq. Milliy birlikni mustahkamlash – bu bizning rivojlanish strategiyamizning asosiy tamoyillaridan biridir.”.[3]

Foydalanilgan adabiyotlar ro‘yxati:

1. Dorothy Dening “Informational Warfare and security” (1998) “Addison Wesley” nashriyoti.
2. Don B.Parker “ Fighting computer crime” (1998) “John Willey&Sons” nashriyoti
3. Mark Goodman “ Future crime “ (2015) “Doubleday” nashriyoti
4. Mirziyoyev Sh.M “ Yangi O‘zbekiston strategiyasi” (2021-yil)
“Toshkent”nashriyoti (103-bet)

KIBER JINOYATCHILIKNI OLDINI OLISHDA XALQARO HAMKORLIK MASALALARI

Ikromov Ozodbek Sherzodbek o‘g‘li
Ilmiy rahbar: yu.f.d.(PhD) I.Atamirzayev

Namangan davlat universiteti Yuridik fakulteti 1- bosqich talabasi

Anotatsiya. Ushbu maqola bugungi kundagi eng dolzarb muammolardan biri bo’lgan kiber jinoyatning mamlakatlar miqyosidagi solayotgan xavfi, kiber jinoyatga qarshi kurashishda mamlakatlar hamkorligi va uni oldini olish maqsadida qilinayotgan sa’y-harakatlar haqida ma’lumot berilgan.

Kalit so‘zlar: kiber makon, kiber hujum, kiber jinoyat, hakker, kiberxavfsizlik.

Hozirgi kunda texlogiyalar taraqqiy etayotgan bir davrda, kiber xavfsizlik masalasi eng asosiy mavzulardan biri bo'lib qolmoqda. Ayniqsa dunyo hamjamiyatidagi aloqalar masalasi bo'yicha kiber jinoyatlar eng ommalashgan davrda turibmiz. Bunday jinoyatlar mamalakatalar o'rtasidagi siyosiy, madaniy, iqtisodiy va boshqa aloqalarga jiddiy putur yetkazishi mumkin. Shuning uchun mamalakatlar birlashib kiber xavfsizlik masalasi bo'yicha yangicha yondashuvlar qilmoqlari zarurdir. Agar bunday kiber jinoyatlar oldini olish masalasi bo'yicha yangicha vositalarni qo'llamasa ular o'rtasidagi aloqalarga ta'sir ko'rsatishi aniq. Hozirgi kunda bu jinoyatlarga kurashish har doimgidanda dolzarb bo'lib qolmoqda.

Kiber makon - bu axborot texnologiyalari va internet tarmog‘i asosida shakllangan virtual muhit bo‘lib, unda ma’lumotlar saqlash, ulashish, o’zaro aloqa qilish va boshqarish jarayonlari amalga oshiriladi.

Hozirgi davrda fan, texnika va asosan kompyuter taraqqiyoti mahsuli bo’lgan kiber makon va uning boshqaruvchi qiyofasi «superkorporatsiya» texnologiyalarning insoniylikdan begonalashuvi natijasida din niqobidagi ijtimoiy va madaniy buzg’unchilikni sodir etishga bo’lgan urinishlar tobora kuchayib bormoqda. Jumladan, bugungi kunda kiber terrorchilik tuzilmalari o’z g’arazli maqsadlari yo’lida axborot-kommunikatsiya texnologiyalaridan keng foydalanishga urinmoqda.

Taassufki, ba’zan islom dini va diniy aqidaparastlik tushunchalarini bir-biridan farqlay olmaslik yoki g’arazli maqsadda ularni teng qo’yish kabi holatlar ham ko’zga tashlanmoqda. Shu bilan birga, islom dinini niqob qilib, manfur ishlarni amalga oshirayotgan mutaassib kuchlar hali ongi shakllanib ulgurmagan, tajribasiz, g’o’r

yoshlarni o’z tuzog’iga ilintirib, boshini aylantirib, ulardan o’zining nopok maqsadlari yo’lida foydalanmoqda. Bunday nojo’ya harakatlar avvalo muqaddas dinimizning sha’niga dog’ bo’lishini, oxir-oqibatda esa ma’naviy hayotimizga salbiy ta’sir ko’rsatishini barchamiz chuqur anglab olishimiz va shundan xulosa chiqarishimiz zarur.[1]

Kiber hujum kompyuter axborot tizimlari, kompyuter tarmoqlari, infratuzilmalar yoki shaxsiy kompyuter qurilmalariga qaratilgan har qanday hujumkor xatti-harakat. Hujumni amalga oshiruvchi shaxs ma’lumotlarga, funksiyalarga yoki tizimning boshqa kirish cheklangan joylariga ruxsatsiz, yomon niyatda kirishga harakat qiladi. Kontekstga qarab kiber hujumlar kiber urush yoki kiber terrorizmga bo‘linishi mumkin. Kiber hujumlar soni biz ularga qarshi kurashish qobiliyatimizga qaraganda tezroq rivojlanmoqda.

Kiber jinoyat kompyuter va tarmoqning birgalikdagi aloqasi ostida sodir etiluvchi jinoyat turi. Kompyuter jinoyat paytida maqsadli yo‘naltirilgan qurol vazifasini bajarib beradi. Kiber jinoyat kimningdir xavfsizligi va moliyaviy bazasiga zarar yetkazish maqsadida sodir etiladi. Bunday jinoyatchilar hakerlar deyiladi.

Haker informatsion texnologiyalar bo‘yicha favqullotda malakaga ega mutaxassis bo’lib,kompyuter sistemasini o‘ta chuqur biladigan shaxs. Dastlab haker degan atama kompyuter dasturlarini tezda yoza oladigan va kompyuterda tez ishlay oladigan dasturchilarga nisbatan ishlatilgan.

2014-yilda chop etilgan McAfee hisobotida jahon iqtisodiyotiga yetkazilgan yillik zarar 445 milliard dollarni tashkil qilgan.

Cyber security Ventures tomonidan 2016-yilgi hisobotda kiber jinoyatlar natijasida yetkazilgan global zararlar 2021-yilga kelib yiliga 6 trillion dollargacha, 2025-yilga kelib esa 10,5 trillion dollargacha ko‘tarilishi bashorat qilingan edi.

2012-yilda AQShda onlayn kredit va debet kartalaridagi firibgarlik oqibatida taxminan 1,5 milliard dollar yo‘qotilgan.

2018-yilda Strategik va xalqaro tadqiqotlar markazi tomonidan McAfee bilan hamkorlikda o‘tkazilgan tadqiqot shuni ko‘rsatadiki, har yili global YaIMning yani Yalpi ichki mahsulotning qariyb bir foizi, ya’ni 600 milliard dollarga yaqini kiber jinoyatlar tufayli yo‘qoladi.

Jahon Iqtisodiy Forumi 2020 Global Risk hisobotida uyushgan kiberjinoyatlar idoralari jinoiy faoliyatni onlayn qilish uchun kuchlarni birlashtirayotganini tasdiqladi, shu bilan birga ularning aniqlash va jinoiy javobgarlikka tortilish ehtimoli AQShda 1 foizdan kamroqni tashkil qiladi.

2024 yilga kelib, kiber jinoyatlardan moliyaviy yo'qotishlar deyarli 70% ga etadi. Juniper Research tadqiqotchilarining fikriga ko'ra, zarar har yili o'rtacha 11 foizga oshadi va 2024 yilga kelib 5 trillion dollardan oshadi. O'tgan yili mutaxassislar kiber jinoyatlardan etkazilgan zararni 3 trillion dollarga baholashgan.[3]

Kiber jinoyatchilikni oldini olishda xalqaro hamkorlik bu hozirgi kunda dolzarb masalalardan biriga aylanishga ulgurdi. Chunki bu turdagi jinoyat milliy va hududiy chegaralarni tan olmaydi. Kiber jinoyatchilar global miqyosda ya’ni butun dunyo bo‘yicha faoliyat yuritadi va turli mamlakatlarning infratuzilmasiga zarar yetkazishi

yoki qonuniy cheklovlardan qochishi mumkin. Kiber jinoyatchilikni oldini olishda xalqaro hamkorlikning asosiy yo‘nalishlari quyidagicha ifodalanadi.

Yana bir muhim hujjatlardan biri bu-Interpolning kiber jinoyatchilik dasturi bo‘lib, bu dastur orqali Interpolga a’zo davlatlar o‘rtasida ma’lumotlar almashish va birgalikda operatsiyalar o‘tkazishga yordam beradi.

Xalqaro hamkorlik ma’lumotlar va texnologiyalar bo‘yicha o‘zaro tezkor almashishni taqozo etadi. Masalan: CERT tarmoqlari orqali turli mamlakatlar kiber tahdidlar haqida tezkor ma’lumot almashadi.Europol va Interpol kabi tashkilotlar global miqyosda kiber jinoyatchilar faoliyatini kuzatadi.

Xalqaro kiber hujumlarni bartaraf etishda davlatlar va xalqaro tashkilotlar birgalikda maxsus operatsiyalar o‘tkazadi. Bunda jinoyatchini ya’ni hakkerni aniqlash,qo’lga olish va jazo qo’llash osonroq va tezroq bo’ladi.

Kiber xavfsizlikni ta’minlash uchun mamlakatlar bir-biriga texnik treninglar va ekspertiza bo‘yicha yordam beradi. Bu orqali davlatlar zamonaviy texnologiyalar va uslublar haqida ma’lumotga ega bo‘lishadi.

Hozirgi kunda barcha davlatlar rahbarlari va xavfsizlik tizimi rahbarlari kiber jinoyatni kamaytirish maqsadida turli xil loyihalar ishlab chiqmoqda va O’zbekistonda ham Prezidentimiz Sh.M.Mirziyoyevning tashabbusi bilan Xavfsizlik tizimini tubdan takomillashtirishga qaratilgan takliflar va loyihalar taklif qilinmoqda.

Ushbu takliflarda kiber jinoyatlarni kamaytirish uchun avvalo qonunchilikni mustahkamlash ya’ni kiber jinoyatlarga doir qonunlar va jarimalarni, sanksiyalarni kuchaytirish lozimligi va bu bilan jamiyatdagi insonlar ongida shu jinoyatni qilishga nisbatan qo’rquv paydo bo‘lishiga olib kelishiga xizmat qilishi ta’kidlandi.

Bundan tashqari monitoring tizimini joriy qilish kerak.Bunda huquqni muhofaza qiluvchi organlarda kiber jinoyatga qarshi kurashish uchun maxsus bo‘limlarni tashkil qilish lozim.

Xalqaro hamkorlikni yo’lga qo‘yish ya’ni kiber jinoyatchilar asosan xalqaro miqyosda faoliyat yuritadi.Shuning uchun bu muammoni xalqaro miqyosda hal qilish uchun davlat o‘rtasida hamkorlikni yanada kuchaytirishga qaratilgan chora-tadbirlarni kuchaytirish va bunday hamkorliklarni qo‘llab-quvvatlash zarur.

Yana bir muhim tadbirlardan biri kiber xavfsizlik tizimlarini takomillashtirish, ma’lumotlarni shifrlash, tahlil va kuzatuv tizimlarini rivojlantirish va ma’lumotlar xavfsizligini ta’minlash zarur.

Xulosa qilib aytganda, kiber jinoyatchilikni oldini olishda xalqaro hamkorlik davlatlar va tashkilotlarga global miqyosda xavfsizlikni mustahkamlash, jinoyatchilarni javobgarlikka tortish va muammoga tizimli yechimlar topishda yordam beradi. Shu bilan birga, global standartlarni ishlab chiqish va ularni amalda qo‘llash xalqaro hamkorlikning muvaffaqiyatini ta’minlaydi.

FOYDALANILGAN ADABIYOTLAR:

1. Karimov.I.A.Yuksak ma’naviyat-yengilmas kuch. Ma’naviyat.T.—2008-yi
2. Jahon Iqtisodiy Forumi 2018-yilgi hisobotida
3. Kiber xavfsizlik markazi .csec.uz.2024
4. Computer Emergency Response Teams

KIBERJINOYATLARNI OLDINI OLISHDA OMMAVIY AXBOROT VOSITALARINING O‘RNI

Nabiyev Abdulloh Nizomjon o‘g‘li
Ilmiy rahbar: yu.f.d.(PhD) I.Atamirzayev

Namangan davlat universiteti Yuridik fakulteti 1-bosqich talabasi

Annotatsiya. Ushbu maqolada bugungi kunda ommaviylashib borayotgan hamda yuqori darajada zarar yetkazayotgan kiberjinoyatning huquqiy oqibatlari hamda unga qarshi kurashishda ommaviy axborot vositalarini muhimligi hamda kiberjinoyatni oldini olishdagi raqamli vositalardagi takliflar va jihatlar tadqiq etilgan. Tadqiqotda analiz - sintez hamda huquqiy metodlardan qo‘llanilgan.

Kalit so‘zlar: Ommaviy axborot vositalari, televideo, radio, teleshou, informatsion tarmoqlar, kiberjinoyat, sanksiyalar va xakerlar, kredit kartalar.

Globallashuv davrida, dunyoda texnikalarning rivojlanishi jadallik bilan o‘sib bormoqda va shu bilan birga uning ba’zi - bir salbiy oqibatlari ham kelib chiqmoqda. Hozirgi kunda ommalashib borayotgan jinoyatlardan biri kiberjinoyatchilik ham davlat va jamiyat xavfsizligiga jiddiy tahdid solayotganligi bilan dolzarbdir.

Ushbu muammoga qarshi kurashish va unga yechim izlashda ommaviy axborot vositalarining ro‘li muhim. Chunki kiberjinoyat nafaqat davlat va jamiyatga balki millatga ham xavf solayotgan muammolardan biridir hamda bu raqamli tarmoqlar sharoiti rivojlangani sari ortib bormoqda.

Kiberjinoyatchilik - kompyuter, kompyuter tarmog‘i va boshqa texnika vositalaridan yoki tarmoq qurilmasidan suiiste’mol qilishga qaratilgan jinoiy faoliyat hisoblanadi. Ularning aksariyati kiberjinoyatchilar yoki xakerlar tomonidan undan noqonuniy daromad orttirish maqsadida sodir etiladi. Bugungi kun ta’biri bilan aytganda, qancha texnologiyalar rivojlangani sari jinoyatchilar ham ulardan foydalanib, noqonuniy xatti-harakatlarni sodir bo‘lmoqda. Bunga misol tariqasida hozirgi kunda ommalashib borayotgan kiberjinoyatlardan biri hisoblangan odamlar plastik kartalaridan pul mablag‘lari noqonuniy tarzda yechib olish sezilarli darajada oshib bormoqda. Tabiiyki, huquqni muhofaza qiluchi organlar tomonidan bu jinoyatlarni oldi olinmoqda va yetkazilgan zararlar to‘laligicha qoplanib berilmoqda.

Hozirgi kunga kelib, kiberjinoyatchilikning turli shakllari shakllanmoqda, ularning huquqiy oqibatlari ham o‘ziga xos jihatlarga ega. Kiberjinoyatchilik bir necha yo‘nalishlarga ajraladi va ular ko‘pincha ommaviy axborot vositalari bilan bevosita bog‘liqdir.

Jumladan, moliyaviy aldov–bu internet orqali bank kartalari, hisob raqamlari yoki onlayn to‘lov tizimlariga noqonuniy ravishda kirib, mablag‘larni talon-toroj qilish hamda soxta e’lonlar orqali foydalanuvchilarni chalg‘itishni o‘z ichiga oladi.

Identifikatsiya ma’lumotlarini talon-taroj qilish, shaxsga oid maxfiy ma’lumotlarni ya’ni shaxsi tasdiqlovchi hujjat, ijtimoiy tarmoqdagi parollarni o‘g‘irlash va ularni noqonuniy maqsadlarga qo‘llash bilan bog‘liq huquqbuzarliklar hisoblanadi.

2022-yilda Toshkentda axborot texnologiyalari yordamida 4332 ta va 2021-yilga (2281 ta) nisbatan qariyb 2 barobar 2020-yil bilan (106 ta) taqqoslaganda esa 40 barobar ko‘p kiberjinoyat sodir etildi”[1].

Bu ko‘rsatgichlar kundan-kun va yildan-yilga oshib bormoqda. Bu sonlarni kamayishi uchun odamlarda doimiy ravishta ogohlik va ehtiyotkorlik masalalariga jiddiy qarashlari so‘raladi. Chunki deyarli barcha jabhalarda ommaviy axborot vositalarida unga qarshi qattiq choralar ko‘rilmoqda qayerga va qaysi internet tarmoqlariga kirib bormang kiberjinoyatlarga qarshi kurash masalasi ilgari surulmoqda, bunga misol tariqasida turli xil ommaviy axborot vositalari orqali ko‘rsatuvlari va gazetalarda ogohlantirishlar berilmoqda.

Turli saytlarga kirish va o‘zlarining shaxsiy ma’lumotlari yuzasidan ochiq malumotlar berilishiga va ularni o‘sha saytning ma’lum bir joylariga kiritishda ehtiyotkorlik so‘raladi.

Kiberjinoyatlarga bog‘liq yana bir global statistikalarni ko‘rsak, 2024-yilning ikkinchi choragida kiberhujumlar soni 30% ga oshgan va har hafta bitta tashkilotga o‘rtacha 1636 hujum qilingan.

Eng ko‘p hujum qilingan sohalarga ta’lim va tadqiqot 3341 ta, davlat va harbiy sohada esa 2084 ta va sog‘liqni saqlash sohasida esa 1095 ta hujumlar sodir etilgan va bularning bir hafta ichidagi sonlardir davlatimiz rahbari qarorlarida shunday deganlar “2024-2025 o‘quv yilidan boshlab raqamli texnologiyalar sohasida jinoyatlarning oldini olish bo‘yicha bosqichma-bosqich kadrlar tayyorlaydigan oliy ta’lim muassasalarini belgilash va ushbu ta’lim yo‘nalishi bo‘yicha kadrlar tayyorlash kvotalarini davlat buyurtmasiga asosan davlat oliy ta’lim muassasalariga o‘qishga qabul qilishning har yilgi davlat buyurtmasi parametrlarini belgilashda inobatga olish”[2] va shu sohaga qarshi ishlarga turtki bo‘lgan desak adashmaymiz.

2023-yil to‘lov firibgarliklari global biznesga 343 milliard dollar zarar yetkazilishi pragnoz qilingan edi. Tashkilotlarning o‘rtacha buzilish aniqlash uchun 197 kun, to‘liq bartaraf etish uchun esa 69 kun talab qilinadi. Eng ko‘p hujumlar Afrika va Lotin Amerikasi davlatlariga uyishtirilgan.

Qo‘shimcha qiladigan bo‘lsak, dunyo bo‘ylab har yili 500 milliondan ortiq kiber hujumlar uyushtiriladi. Har soniyada 12 nafar insondan biri kiber makonda sodir etilgan hujumlar qurboniga aylanadi. Amerika Qo‘shma Shtatlari, Fransiya, Angliya, Germaniya, Belgiya, Luksemburg kabi rivojlangan davlatlarda jinoyatlarning 60-65 foizi kiber hujumlar orqali sodir etilmoqda.

O‘zbekistonda ham so‘nggi uch yilda bu turdagi jinoyatlar 8,3 baravarga ko‘payib, hozirda umumiy jinoyatchilikning qariyb 5 foiziga yetgan. Xususan, noqonuniy bank-moliya operatsiyalari orqali o‘zgalarning plastik kartadagi mablag‘larini o‘zlashtirish, zararli viruslar tarqatish, qimor va tavakkalchilikka asoslangan onlayn o‘yinlar, diniy aqidaparastlikka qaratilgan axborot xurujlari, onlayn savdo maydonidagi firibgarlik jinoyatlari ko‘payib bormoqda.

Mamlakatimizda axborot xavfsizligi masalasiga davlat siyosati darajasida e’tibor qaratilib, kiberjinoyatchilikka qarshi kurashishning yangi yondashuvlari amaliyotga joriy qilinmoqda, – dedi IIV Akademiyasi boshlig‘i Rustam Xatamov.

Chunki virtual olamdagi jinoyatlarning zarari va xavfi real olamdagi tahdiddan oshib borayotganiga guvoh bo‘layapmiz. Bu borada “Kiberxavfsizlik to‘g‘risida”gi

yangi qonunning qabul qilinayotgani sohani davlat tomonidan tartibga solishga, mamlakatimiz axborot tizimlari va tarmoqlariga noqonuniy aralashishning oldini olishga xizmat qiladi.

Bunga qo‘shimcha sifatida deyarli barcha narmativ hujjatlarda shu qatori ma’muriy kodeks, jinoyat kodeksi va bashqa xalqaro hujjatlarda kiber hujumga qarshi turli xil sanksiyalar mavjud. Xalqaro doiradan olganda ko‘plab tashkilotlarga aynan kiberjinoyatlar bilan boğliq masalalar yuklatilgan bularga misol qilib ba’zi tashkilotlarni kiritish mumkin.

Birinchi navbatda Birlashgan Millatlar Tashkiloti (BMT)ning turli bo‘linmalari, masalan, BMTning Iqtisodiy va Ijtimoiy Kengashi (ECOSOC) va BMTning Kiberxavfsizlik bo‘yicha maxsus guruhi, global miqyosda kiberxavfsizlikni rivojlantirishga qaratilgan tashabbuslarni qo‘llab-quvvatlaydi.

Ikkinchi navbatda Evropa Kiberxavfsizlik Agentligi (ENISA) Evropa Ittifoqining kiberxavfsizlikni ta’minlashga yo‘naltirilgan agentligi bo‘lib, mamlakatlar o‘rtasida kiberxavfsizlikni yaxshilash bo‘yicha hamkorlikni rivojlantiradi.

Ertangi jinoyatlarni oldini olish uchun va ularning ildizini quritish uchun juda ham ko‘p qo‘shimcha va o‘zgartirishlar kerak, ya’ni ommaviy xabarlikni oshirish kerak ya’ni bu qanday amalga oshiriladi, bu sohada turli intervyularni, maqolalarni va infagrafikalarni berib borishdir.

Bundan ko‘zlangan asosiy maqsad insonlarga bu jinoyatlarni turlarini va ularni amalga oshirilganda javobgarlikni keltirib chiqarishi va jazolarni amalga oshirilishi haqida xabar berish tushuniladi. Bu masalaga qarshi kurashishda faqat davlat va uning organlari emas balki odamlarning o‘zlari ham harakat qilishi so‘raladi,ya’ni o‘zlarining yaxshi ma’lumotlarini va bank hisoblarini yaratishda ishonchli va xavfsizlik darajasi yuqori bo‘lgan parollardan foydalanishi va bu jarayon ularning kiber hujumlardan saqlanishida foyda berishi haqida tushunchalarni doimiy ravishda e’lon qilinishi kerakligini anglatadi.

Ta’lim sohasida ham turli treninglar o‘tkazish va maxsus dasturlarni yaratish ya’ni ommaviy axborot vositalari orqali bolalar, ota-onalar va biznes sohasidagi kishilar uchun onlayn xavfsizlik bo‘yicha maxsus video darslar va treninglarni tashkil etish hamda aholi orasida savodxonlikni oshirish uchun tanlovlar, viktorinalar va jonli muloqotlar o‘tkazish, shu jinoyat va shu bilan boğliq jinoyatlar bilan jabrlangan qurbonlar, shu sohadagi mutaxasislar va huquq- tartibot organlarini radio, teleshou va ko‘pchilik foydalanadigan saytlarda kiberjinoyatga qarshi tashviqot ishlari va o‘sha jarayonlar aks etgan videoroliklarni joylab borishi hamda eshittirishlarda o‘sha massalalarning oqibatlarini keng miqyosda e’lon qilinishi kerak.

Qo‘shimcha tariqasida shu masala yuzasidagi adabiyotlar bilan tanishish kerak” Kiberjinoyat tahlili,tarmoq hujumlari va razvedka strategiyalari”[3]. Chunki “ Biz texnalogiyaga qancha ko‘proq boğliq bo‘lsak,shuncha ko‘proq xavf ostidamiz”[4] degan so‘zlarni tag zamiriga yetiladi va unga qarshi immunitet paydo bo‘lishi mumkin va bularga mutola qilish orqali erishiladi.

Yuqorida takidlab o‘tilgan masalalar va muammolarni kelib chiqishini oldini olish uchun inson avvalo o‘zining huquqiy onggini yuqori cho‘qqisiga olib chiqishi kerak.

Bularga shiddatli zarba berish uchun ommaviy axborot vositalaridan foydalanilanish maqsadga muvofiq deb o‘ylayman chunki hozir texnika rivojlangan davrda biz o‘zimiz hohlaymizmi yo‘ğmi informatsion qurilamalarga duch kelamiz va ular bizni o‘rab olgan shuning uchun ham undagi jarayonlardan xabardor bo‘lamiz va unda nisbatan o‘zimizning salbiy yoki ijobiy fikr va emotsiyalar beramiz va bu orqali hujumlardan saqlanish masalalarini anglab yetamiz.

FOYDALANGAN ADABIYOTLAR:

1. https://www.gazeta.uz/en/
2. Mirziyoyev Sh.M. “Raqamli mahsulotlar iste’molchilari huquqlarini himoya qilish va raqamli texnologiyalar orqali huquqbuzarliklarga qarshi choralar to‘g‘risidagi qarori” PQ-381-son, 30-noyabr, 2023.
(https://lex.uz/docs/-6681111?otherlang=1)
3.Jon R.B. “ The Art of Cyber War”15.07 2022.
4.Mars G.“ Future Crimes”24.02.2015.

YANGILANAYOTGAN O‘ZBEKISTONDA KIBER JINOYATLARGA QARSHI KURASHISHNING O‘ZIGA XOS JIHATLARI

Rayimov Mirjalol Xusan o‘g‘li
Ilmiy rahbar: yu.f.d.(PhD) I.Atamirzayev

Namangan davlat universiteti Yuridik fakulteti 1-boshqich talabasi

Annotatsiya. Mazkur maqolada Yangi O‘zbekistonda kiber jinoyatlarga qarshi kurashishning zamonaviy usullari va vositalari, hamda jinoyatlarni oldini olish bilan bog‘liq turli islotlarni tizimli ravishda amalga oshirishning samarali yo‘llari, hamda shu jinoyatlarga qarshi kurashishga oid takliflar va talablar haqida fikr yuritilgan.

Kalit so‘zlar: kiberjinoyatchilik, kiber makon, kiber jinoyatlar, kiber hujum, xakerlik, fishing, kiberfiribgarlik, ijtimoiy tarmoqlar.

Hozirgi zamonda globallashuv jarayonida butun dunyoda jahon internet tarmoqlari juda jadallik bilan rivojlanib bormoqda. Bu rivojlanish O‘zbekistonni ham chetlab o‘tgani yo‘q. Buning foydali taraflari juda ko‘plab topishimiz mumkin, lekin bu aynan kiber makonda hozirgi globallashuv bilan bir qatorda turli xil kiber jinoyatlar sodir etilmoqda.

So‘nggi paytlarda ijtimoiy tarmoqlarda turli xil virusli dasturlar jo‘natish va ularni buzib kirish keng tarqalgan.Kiber jinoyatlar o'tgan yillarda sodir bo‘lgan pandemiya davrida jiddiy muammolardan biriga aylandi va hozirgi kunda ham dolzarb mavuzligicha qolmoqda. Bunga yechim topish hozirgi kunning dolzarbligi yuqori mavzularidan biri bo‘lmoqda.

Kiber jinoyatlar - bu kompyuter tarmoqlari yoki internetdan foydalanib sodir etiladigan huquqbuzarlik bo‘lib, unda texnologiyalar vositasida shaxsiy, korporativ yoki davlatga tegishli axborot, moliyaviy resurslar yoki boshqa obyektlarga noqonuniy ravishda zarar yetkaziladi.

Axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik

vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi. Kiber jinoyatlar kimningdir xavfsizligi va moliyaviy saviyasiga zarar yetkazish maqsadida sodir etiladi.

Kiberjinoyatchilik bu - kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat turi bo‘lib, uning eng keng tarqalgan turlari - kompyuter qaroqchiligi, onlayn firibgarlik, kompyuter tizimlariga hujum qilish, shaxsiy ma’lumotlarni o‘g‘irlash va noqonuniy yoki taqiqlangan ma’lumotlarni tarqatish.[1][1]

Kiber makon - axborot texnologiyalari yordamida yaratiladigan sun’iy muhitdir. Kiber jinoyatlar bir necha turlarga bo‘linadi: ma’lumotlarni o‘g‘irlash va buzish, moliyaviy jinoyatlar, pornografik va noqonuniy kontentlarni tarqatish, ijtimoiy tarmoqlardagi jinoyatlar, davlat va korporativ boshqaruv tizimlariga hujum va boshlarni misol qilishimiz mumkin.

Ma’lumotlarni o‘g‘irlash va buzish - bu kiber jinoyatlarchilar tomonidan shaxs va fuqarolarning shaxsiy ma’lumotlarini ruxsatsiz olish va ularni tarqatishdir.

Xakerlik - himoyalangan tizimni buzib kirish

Fishing - soxta saytlar yoki xabarlar orqali insonlarning o‘ziga tegishli bo‘lgan shaxsiy ma’lumotlarini o‘g‘irlash.

Moliyaviy jinoyatlar - bu davlatga yoki fuqarolarga va shaxslarga tegishli bo‘lgan mulklarni ularning iqtisodiy faoliyatiga zarar yetkazish orqali amalga oshiriladi.

Ularning eng keng tarqalgan turlaridan biri bu kiber firibgarlikdir.

Kiberfiribgarlik - internet orqali insonlarni aldash yo‘li bilan undiraligan to‘lov vositasi.

Pornografik va noqonuniy kontentlarni tarqatish - bu turli xil saytlarda yoshlarning ongini zaharlashga qaratilgan va qonunchilikka zid bo‘lgan ma’lumotni tarqatishdir. Zo‘ravonlikni taqib qiluvchi kontentlar - zo‘ravonlik, odam savdosi, jinsiy ekspluatatsiyani targ‘ib qiluvchi ma’lumotlarni saqlash, tarqatish va ulashishdir.

Ijtimoiy tarmoqlardagi jinoyatlar - bu har xil kiber makonlarda insonlarni tahqirlash yoki ularni kamsitish bilan ularga ruhiy va ma’naviy zarar yetkazish va shaxslarning o‘zlariga tegishli bo‘lgan shaxsiy ma’lumotlarini ruxsatsiz oshkor qilish tushuniladi.

Davlat va korporativ boshqaruv tizimiga qarshi kiber jinoyatlar - davlat sirlarini o‘g‘irlash, oshkor qilish, davlat xavfsizlik tizimlarini buzib kirish ularni ishdan chiqar va uning aholisini qo‘rqitish maqsadida kiber hujumlar uyushtirish.

Bugungi kunda kiber jinoyatchilar tomonidan sodir etilayotgan jinoyatlar davlat va uning fuqarolari yoki boshqa shaxslarning xavfsizligiga putur yetkazmoqda. Bunga misol qilib turli yillardagi statistik ma’lumotlarni olsak , ularda yildan yilga o‘sish kuzatilmoqda.

Buni dunyo misolida kuzatsak, 2024 yilga kelib, kiber jinoyatlardan moliyaviy yo'qotishlar deyarli 70% ga etadi. Juniper Research tadqiqotchilarining fikriga ko'ra, zarar har yili o'rtacha 11 foizga oshadi va 2024 yilga kelib 5 trillion dollardan oshadi. O'tgan yili mutaxassislar kiber jinoyatlardan etkazilgan zararni 3 trillion dollarga baholashgan.

Endi davlatlardagi kiberjinoyatchilikka nazar solsak, Rossiya federatsiyasining Moskva shahrining o‘zida 2020-yil ma’lumotlariga nazar solsak bu ko‘rsatkich 102 060 ta kiberjinoyatchilik qayd etilgan.

Lekin 2021-yil bu ko‘rsatkich 103 600 tani tashkil qiladi. Seul ya'ni Janubiy Koreya poytaxtida bu ko‘rsatkichlar 2021-yilda 56 210 tani tashkil etmoqda , lekin bu ko‘rsatkich 2022-yil 60 450 ta kiberjinoyatchilik sodir etilgani aniqlangan. Bunday kiberjinoyatchilik O‘zbekistonning poytaxti Toshkentdagi ko‘rsatkichlar yillar davomida oshib bormoqda.

2021-yilda Toshkentda axborot texnologiyalari yordamida 2281 ta kiberhujum uyushtirilgan. 2022-yilda esa bu kiberjinoyatchilik ko‘rsatkichi 4332 tani tashkil etadi. Bu ko‘rsatkich qariyb 2 barobar ko‘paygani ko‘rishimiz mumkin. Bu jinoyatlarning 3372 tasi yoki 82 foizi bank plastik kartalarini talon-taroj qilish bilan bog‘liq. Kiberjinoyatchilikdan Toshkent shahar aholisi 2022-yilda 45,2 mlrd zarar ko‘rgan.

Ushbu jinoyatlarni oldini olishda davlat huquqni muhofaza etuvchi organlar tomonidan turli xil zamonaviy usullari amalga oshirilmoqda. Xususan, qonunchilikni mustahkamlash va takomillashtirish, fuqarolarni xabardor qilish va xalqaro hamkorlik qilish kabi ishlar amalga oshirilmoqda.

Qonunchilikni mustahkamlash ya'ni jinoyat kodeksida kiberjinoyatchilikni oldini olish bo'yicha chora-tadbirlarni amalga oshirish bo‘yicha moddalar qo‘shilishi va ularni sodir etgan shaxslarga nisbatan jazo turlarini joriy qilish, hamda shaxslarning ma’lumotlar xavfsizligini ta’minlash uchun "Elektron hukumat" va "Shaxsiy ma’lumotlar to‘g‘risida"gi qonunlar qabul qilingan.

Fuqarolarni xabardor qilish bu mas’ul davlat organlari tomonidan shaxslarga beriladigan kiberjinoyatchilik haqida qimmatli ma’lumotlar.

Bu ma’lumotlar qanday qilib jinoyatchilarning aldovlariga aldanmaslik, soxta xabarlarga aldanmaslik va shunday holat sodir bo‘lgan taqdirda tuman yoki shahar IIBsiga murojaat qilishi so‘raladi kabi ma’lumotlarni yetkazib berish ma’sul xodimlar tomonidan amalga oshiriladi.

Bu borada IIB Axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurashish boshqarmasi tergov bo‘limi boshlig‘i Anvar To‘xtayev shunday degan edi: “Aholi bilan olib borilgan keng qamrovli profilaktik chora-tadbirlarga qaramasdan, bu turdagi jinoyatlarning salmog‘i yuqoriligicha qolmoqda. Aholimiz hanuzgacha buni tushunib yetganicha yo‘q. Bu turdagi jinoyatlarning o‘ziga xos jihatlari shundaki, birinchidan, axborot texnologiyalari sohasida sodir etilayotgan jinoyatlar hudud, chegara va makon tanlamaydi. Ikkinchidan, birgina harakat bilan bir nechta fuqarolarga moddiy zarar yetkazishi mumkin. Uchinchidan, jinoyatlar yuqori texnologiyali, modifikatsiya qilingan dasturlardan foydalangan holda sodir etilmoqda”2[] .

Dunyo hamjamiyati bilan birgalikda bu kiberjinoyatchilikga qarshi kurashishga qarshi turli xil nizomlar, yo‘riqnomalar va boshqa normativ-huquqiy hujjatlar qabul qilingan.

2001-yilda qabul qilingan Budapesht konvensiyasi. Bu konvensiyasiyaning asosiy maqsadi davlatlar o‘rtasidagi kiberjinoyatchilikni tergov qilish va sud jarayonlarini osonlashtirish uchun hamkorlikni ta’minlash. Bu konvensiya kiber jinoyatlarga qarshi kurashishda eng muhim manba bo‘lib xizmat qiladi. Undan so‘ng BMTning "Kibermakon va kiberxavfsizlik bo‘yicha rezolyutsiyasi".Bu

rezolyutsiyaning maqsadi kiberjinoyatchilikning oldini olish va dunyo bo‘ylab kiber xavfsizlikni ta’minlashga yo‘naltirilgan. Va boshqa normativ-huquqiy hujjatlarni misol qilishimiz mumkin.

"Kiberxavfsizlik texnologiyalari qanchalik rivojlangan bo‘lmasin, ularning samaradorligi ko‘pincha insonlar o‘zlarini qanday tutishiga bog‘liq. Kiberjinoyatchilikka qarshi kurashning birinchi qadami — xodimlarni xabardor qilish va ularga xavfsiz xatti-harakatlar odatini singdirishdir."[3]

Bu jumlada kiber jinoyatlarga qarshi kurashish vositasi sifatida inson omili tanlangan. Inson o‘z huquqiy ongini rivojlantirib, uni boshqalarga ham o‘rgatsa, mana shunday kiber jinoyatlar to‘riga ilinib qolmaydi .

“Kiberjinoyatchilikka qarshi kurashda samarali strategiya uch asosiy tamoyilga tayanadi: aniqlash, to‘sqinlik qilish va javob choralarini ko‘rish. Hujumlar doimo yangi usullar bilan amalga oshiriladi, shu sababli xavfsizlik tizimlarini doimiy ravishda yangilab borish lozim.”[4]

Mazkur jumlada asosiy 3ta tamoyillari aytib o‘tilgan. Bu fikrlar albatta to‘g‘ri, kiber jinoyatlarni aniqlash lozim, aniqlangandan so‘ng ularga to‘sqinlik qilinadi va so‘nggi chora sifatida jazo chorasi qo‘llaniladi.

Hozirgi dunyoda texnologiyalar juda jadal sur’atlarda rivojlanmoqda va buning natijasida kiber jinoyatlar ham juda jadal o‘smoqda. Buning oldini olish maqsadida tepadagi fikrga muvofiq xavfsizlik tizimlarini doimiy ravishda yangilab bormoq zarurdir.

Bu yangilanishlar albatta davlatning o‘ziga foydadir, chunki kiber jinoyatlarchilar davlatning maxfiy ma’lumotlarini o‘g‘irlasholmaydi, qachonki xavfsizlik tizimi ancha takomillashgan va dunyo standartlariga mos kelgan taqdirda .

Bunday qilmish qilgan shaxslarga shunday jazolar berilishi kerakki bunday jinoyatlarga boshqa qo‘l urmasin. Jinoyat kodeksida kiberjinoyatchilik sodir etgan shaxslarga nisbatan jazo choralari qo‘llangan.

Axborot tizimlariga noqonuniy ravishda kirish va bunga yengil holatda jarima to‘lash, og‘ir holatlarda esa 3-yilgacha ozodlikdan mahrum qilish jazosi tayinlanadi.

278-moddasida Kompyuter axborotlarini noqonuniy ravishda o‘zlashtirish yoki yo‘q qilish. Yengil holatda 2 yilgacha axloq tuzatish ishlari yoxud jarima bilan cheklanadi. Og‘ir holatlarda esa 3-yilgacha ozodlikdan mahrum qilish jazosi bilan belgilanadi va boshqa huquqiy jazo choralari qo‘llaniladi.

Shunday qilib kiber jinoyatlarga qarshi kurashishning eng muhim usullaridan biri bu inson omili ekan.

Inson o‘z huquqiy ongini rivojlantirib unga amal qilsa kiber jinoyatlarga, soxta habarlarga aldanib qolishmaydi. Shu bilan bir qatorda bunga mas’ul shaxslarning ham zimmasida katta majburiyatlar bordir. Ular xalqga o‘z huquqlarini tushuntirishlari va bu haqida ommaga ma’lum qilishlari kerak va omma bu haqida bilish zarur.

“2024/2025 o‘quv yilidan boshlab kamida bir nafar yetakchi milliy va xorijiy mutaxassisni, ekspert va professor-o‘qituvchilarni raqamli texnologiyalar sohasida jinoyatlarning oldini olishning tashkiliy-texnik yechimlari va bunda sun’iy intellekt texnologiyalarini qo‘llash bo‘yicha kiberxavfsizlik bo‘linmalari xodimlarini o‘qitish, ularning malakasini oshirishda ishtirok etish uchun jalb qilish”.[5]

Bu qarorda shuni ta’kidlayaptiki, davlat tizimlarini yoki boshqa korxonalar tizimlarini yaratishda albatta malakali mutaxassis va kadrlar zarurligi aytib o'tilmoqda va buning uchun xorijdan eng tajribali mutaxassislarni olib kelib o‘zimizning yosh kadrlarimizga shuni o‘rgatishimiz va ularni ham kelajakda sun'iy intellekt texnologiyalaridan juda unumli va oqilona foydalanib davlatga o'zing hissasini qo‘shishi ko‘zda tutilgan.

Yuqoridagi fikrlardan kelib chiqib kiberjinoyatchilikga qarshi kurashishga ba’zi bir takliflarni keltirib o‘tsam:

Birinchidan: Huquqiy jazo choralari kuchaytirish, ya'ni shunchaki jarima qo‘llamasdan ularga ko‘proq jazo qo‘llashni taklif etaman.

Ikkinchidan: Biron bir ma’lumotni ijtimoiy tarmoqlarga joylashda tajribali mutaxassislar yordamidan foydalanish kerak. Buning natijasida kiber jinoyatlar soni ancha kamayishi mumkin.

Uchinchidan: Hozirgi vaqtdagi statistik ma’lumotlarga qaraganda sodir etilayotgan jinoyatlarning 82 foizi bank plastik kartalarini talon-taroj qilish bilan bog‘liq bo‘lganligi sababli, shu bank kartalarini juda maxfiy kodlar bilan chiqarishi kerak deb o‘ylayman.

Chunki eng ko‘p sodir etilayotgan jinoyatlar aynan shu sohadadir.

To‘rtinchidan: Har bir tumandagi IIB hodimlari yoki kiberjinoyatchilikga qarshi kurashish hodimlari o‘sha tumandagi mahalla qo‘mitalariga borib individual yondashishi kerak.

Xulosa sifatida Yangilanayotgan O‘zbekistonda kiber jinoyatlarga qarshi kurashishning eng ustuvor vazifalari sifatida insonlarga ushbu jinoyatlarni tushuntirish hamda ularni oldini olish bo'yicha chora-tadbirlarni amalga oshirishdir.

Bunday kiber jinoyatlar sodir etilar ekan, mamlakat xavfsizligiga va iqtisodiga putur yetkazishi tabiiy holdir. Yana shuni ta’kidlash lozimki, xalq bunday kiberjinoyatchilikdan habari bo‘lmas ekan, jinoyatchilar xalqning pullarini o‘g‘irlashda davom etaveradi.

Bu borada axolimizni huquqiy ongi va huquqiy madaniyatini oshirilsa, ularning AKT foydalanishlari bo‘yicha bilimlari bu kabi jinoyatlar sodir bo‘lmaydi.

FOYDALANILGAN ADABIYOTLAR

1. S.K.G'aniyev, A.A.G'aniyev,S.T.Xudoyqulov, Kiberxavfsizlik asoslari: o‘quv qo‘llanma. — T.: " Aloqachi", 2020, 259 - bet
2. Kevin Mitnik,William L. Simon,Steve Wozniak "The Art of Deception" AQSH 2002.
3. Bruce Schneier — "Secrets and Lies: Digital Security in a Networked World" AQSH 2015.
4. Mirziyoev Sh.M. PQ-381 sonli qarori Toshkent 2023
5. Kun.uz veb rasmiy sayti

ЯНГИЛАНЁТГАН ЎЗБЕКИСТОНДА КИБЕРЖИНОЯТЛАРНИ КЕЛИБ ЧИҚИШ САБАБЛАРИ

Собиров Шамсиддин Хотамбек ўғли
Ilmiy rahbar: yu.f.d.(PhD) I.Atamirzayev

Наманган давлат университети Юридик факултети 1-босқич талабаси

Аннотация. Ушбу мақолада Ўзбекистонда кибер жиноятларнинг келиб чиқиш сабаблари, ўзига хос хусусиятлари шунингдек кибер жиноятларнинг олдини олиш масаласи бўйича амалга оширилаётган кураш чоралари ҳақида фикр юритилган.

Калит сўзлар: кибернетика, ахборот технологиялар, молиявий фирибгарлик, киберҳужум, ахборот хавфсизлиги.

Ҳозирги ривожланаётган даврда технологиялар ва ахборот воситаларининг жадал ривожланиши кибер жиноятларни тез суратда ошишига сабаб бўлмоқда.

Кибер жиноятчилик – ахборот воситалари ва компютер тармоқларидан фойдаланиб амалга ошириладиган жиноят тури ҳисобланади. Кибер жиноят мамлакатнинг иқтисодий, ижтимоий, сиёсий соҳаларига жиддий зарар келтиради.

Ўзбекистон ҳудудида тезкор тартибда ўсиб бораётган жиноят турларидан бири ҳисобланади. Ахборот технологияларига қаратилган жиноятлар асосан шахсларнинг кибернетика, ахборот хавфсизлиги ҳақидаги билимларнинг пастлиги каби **жиҳатлар** бу жиноятни олиб келадиган тамойил бўлиб қолмоқда.

Шунингдек, Ўзбекистонда кибер жиноятчиликка қарши курашиш учун ҳуқуқий нормаларни такомиллаштириш, махсус кибер хавфсизлик марказларини яратиш, илғор технологияларни жорий этиш ва фуқароларни ахборот хавфсизлиги бўйича маълумотлаштириш.

Бу чора-тадбирлар кибер жиноятчиликка қарши самарали курашиш ва мамлакатда ахборот хавфсизлигини таъминлаш учун зарур бўлган асосий қадамлар ҳисобланади. Шунингдек, халқаро ҳамкорликни мустаҳкамлаш ва ахборот технологияларини ривожлантириш орқали кибер жиноятчиликка қарши глобал миқёсда курашишни кучайтириш мумкин.

Шуларни хисобга олган ҳолда, 2003-йил 11-декабрда Ўзбекистон Республикаси Олий Мажлиси томонидан “Ахборотлаштириш тўғрисида” ги қонун қабул қилинди.

Мазкур қонун асосан ахборот технологиялари билан боғлиқ фаолиятни тартибга солади ва ахборот ресурсларнинг хавфсизлигини таъминлайди. Бундан ташқари қонун орқали давлат хизматларига ноқонуний аралашиш таъқиқланди, шунинг натижасида кибер хужумлардан ахоли химоя қилиш сезиларли равишда ошиб бормоқда.[1]

Шундай қонунлар қабул қилнишига қарамай айрим шахслар кибер хужум таъсирига тушиб қолмоқдалар. Албатта бундай холатларни жуда ҳам кўп учратганмиз.

Масалан, Ўзбекистон ҳудудида сўнгги 10 йил ичида кибер ҳужумларнинг сезиларли даражада ўсиши кузатилди.

2022 йилда мамлакатдаги ресурсларга 4,5 миллион, 2023 йилда эса 11 миллиондан ортиқ киберҳужум қайд этилган. Ҳужумларнинг кўп қисми давлат органлари ва молия сектори каби муҳим соҳаларга қаратилган. Айниқса, молиявий фирибгарлик ва зарарли кодларни тарқатиш каби фаолиятлар кўпайгани таъкидланмоқда.

Ушбу даврда давлат ташкилотлари ва бошқа ресурсларга қарши SQL инъексия, DDoS ҳужумлар ва шахсий маълумотларни ўғирлаш каби усуллар кенг қўлланилган.[2]

Юқоридаги фикрларни амалий аҳамияти сифатида киберҳужумлар 2 йил ичида сезиларли тарзда ошганини статистик маълумотлардан кўриш мумкин. Бу жараёнлар шундай давом этса, мамлакат инқирозга учрайди, мамлакатда иқтисодиёт хеч бир жабҳада ўсмай қолади. Бунинг сбабаи сифатида қўйидаги омилларни келтириш лозим.

Биринчидан, инвестицияларнинг қисқариши яъни киберхавфсизлик таъминланмаган мамлакатга халқаро сармоядорлар ишончсизлик кўзи билан қарайди. Киберҳужумлар юзага келиши натижасида сармоялар кетиши ёки янги инвестициялар киритилиши пасаяди.

Иккинчидан, жамоатчилик ишончининг йўқолиши яъни агар давлат ёки хусусий сектор киберхавфсизликни таъминлай олмаса, аҳоли ва мижозлар ташкилотларга бўлган ишончини йўқотади. Бу савдо ва хизматлардан фойдаланишни камайтиради.

Давлатимиз раҳбари Шавкат Мирзиёев 2022-йилда Шанхай Хамкорлик Ташкилотининг саммитида кибер макондаги таҳдидларга карши нутқида, кибер харакатлар ноқонуний мақсадлар, жумладан, экстремизм, ва терроризмни тарғиб қилишда ноқонуний харакатларга алохида эътибор қаратди.

Халқаро минтақада кибермакондаги хавф – хатарларни аниқлаш ва уларга қарши чора кўриш учун махсус экспертлар форумини ташкил қилишни таклифини билдирди.

Бундан ташқари Саммитдаги чиқишида Ўзбекистонда ёшларни киберхавфсизлик соҳасида таёрлаш учун ўқув дастурлар ташкил этилаётгани, шунингдек, ҳар йили кибержиноятлар профилактикаси бўйича танловлар ўтказилиши режалаштирганлиги ҳақида маълумот берди.

Бу ташаббуслар мамлакатнинг рақамли хавфсизликни таъминлашдаги қатъий позициясини кўрсатишни билдирди.

Биз бундай холатлар кўпайган сари кибернетикани олдини олишга қаратилган қонунларга талаб сезамиз, бундай қонунларга талаб ёки зарурат шунга асосланганки, рақамли дунёда хавфсизликни таъминлаш фақатгина давлат, жамият ва шахсий манфаатларни ҳимоя қилиш учун керак бўлади.

Бунинг асосий сабаби: киберҳужумлар аҳоли, иқтисодиёт ва давлат тизимларига катта хавф туғдиради. Қисқача тушунтирганда, ахборот технологиялари соҳасидаги қонунчилик хавфларни олдиндан бартараф этиш, маълумотларни ҳимоя қилиш ва барқарор ривожланишни таъминлаш учун

зарурдир. Ушбу қонунлар маълумотларни ўғирлаш, фирибгарлик, ва давлат суверенитетига таҳдидларни чеклашга қаратилган.

Шундай холатларни инобатга олган ҳолда Ўзбекистонда 2022-йил 15-апрелда “Киберхавфсизлик тўғрисида”ги қонун ишлаб чиқилди.

Бу қонун киберхавфсизлик соҳасидаги муносабатларни тартибга солади ва кибержиноятчиликка қарши курашишнинг умумий тамойилларини белгилайди.

Бу қонун мамлакатда ахборот тизимлари ва тармоқларининг химоясини кучайтириш, давлат идораларида ва корхоналарда киберхавфсизликни таъминлаш талабларини ўрнатиш, киберхужумларни олдини олиш ва уларга қарши чоралар кўришга қаратилган давлат сиёсатини ўрнатади.[3]

Ўзбекистон ҳукумати кибержиноятларни олдини олиш ва уларнинг салбий таъсирини камайтириш учун бир қанча муҳим режалар ва ташаббусларни олдига мақсад қилиб қўйган.

Кибержиноятлар замонавий жамиятга жиддий таҳдид бўлиб, уларнинг олдини олиш учун ҳар томонлама долзарбдир.

Жумладан қуйидагилар ахборот хавфсизлигини таъминлаш, ахборот технологиялари соҳасидаги ривожланиш кибержиноятларни олдини олишга имкониятлар яратмоқда.

Шунингдек ахборот тизимларини ҳимоя қилиш, давлат ва хусусий сектор ташкилотларининг ахборот тизимларида хавфсизлик чораларини кучайтириш, шахсий маълумотларни ҳимоя қилиш, фуқароларнинг шахсий маълумотларини ҳимоя қилиш ва маълумотларнинг ноқонуний фойдаланилишига йўл қўймаслик, кибержиноятлар тўғрисидаги қонунлар, кибержиноятларни барвақт аниқлаш, тергов қилиш ва уларни жазолашга оид қонунлар кучайтириш бугунги куннинг кечиктириб бўлмас вазифа эканлигини билдиради.

Ўзбекистон Республикасининг Жиноят кодекси ва бошқа тегишли қонунларга кибержиноятлар билан боғлиқ нормалар киритилган.

Мазкур жиноятлар ривожлангани сайин санкция қисми хам шу ривожланишга мутаносиб тарзда ўсиб бормоқда.

Бу борада халқаро ҳамкорлик масаласига катта эътибор қаратилиши лозим.

Кибержиноятлар халқаро миқёсда ҳам содир бўлиши мумкин, шунинг учун Ўзбекистон бошқа ривожланган мамлакатлар билан ҳамкорлик алоқаларини ўрнатган.

Бу борада киберхавфсизлик бўйича тарғибот ишларини ўтказиш ҳам мухим аҳамият касб этади.

Фуқароларни киберхавфсизликка оид хатарлар ва ҳимоя чораларига оид нормалар билан хабардор қилиш учун жамоат ташкилотлари ва медиа орқали тарғибот ишлари олиб бориш мухим ҳисобланади.

Бизнингча Ўзбекистонда киберхавфсизлик бўйича танловлар ёки семинар тренинг дарслар ўтказиш, ёшларда киберхавфсизлик ва кибержиноятчилик хақидаги билимларини оширишга қаратилган лойихаларни ўтказиш зарур.

Хулоса сифатида кибер жиноятчиликка қарши курашишда давлат ва жамиятнинг ўзгаришларига мос бўлган қонунчилик, ахборот хавфсизлиги бўйича самарали чоралар ва ёшларга йўналтирилган таълим дастурлари муҳим аҳамиятга эга.

Бу йўналишдаги ташаббусларнинг ҳаётга татбиқ этилиши, мамлакатдаги киберхавфсизликни мустаҳкамлаш ва иқтисодий ўсишни таъминлашга хизмат қилади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Ўзбекистон Республикаси. «Ахборотлаштириш тўғрисида»ги Қонун. 2003-йил 11-декабрь. (https://lex.uz/docs/15519)
2. Ўзбекистонда киберхужумлар: бунинг ортида кимлар туради, мақсад нимада? (https://kun.uz/uz/78649948)
3. Ўзбекистон Республикаси. «Киберхавфсизлик тўғрисида»ги Қонун. 2022-йил 15-апрел. (https://lex.uz/en/docs/-5960604)

KIBERJINOYATLARNI YOSHLAR TARBIYASIGA TA'SIRI

Sotvoldiyev Arabboy Rasuljon o'g'li
Ilmiy rahbar: yu.f.d.(PhD) I.Atamirzayev

Namangan davlat universiteti Yuridik fakultetining 1-bosqich talabasi

Annotatsiya. *Bugungi raqamli dunyoda kiberjinoyatlar jahon miqyosida keng tarqalgan muammo bo'lib kelmoqda va u yoshlar hayotiga ham salbiy ta'sir ko'rsatmoqda. Internetdan foydalanuvchi yoshlarning soni ortgani sari ular nafaqat zararli kontent bilan duch kelmoqdalar, balki o'zlari ham kiberjinoyatlarga aralashib qolish xavfiga yaqindir Ushbu maqolada kiberjinoyatlarning yoshlar tarbiyasiga bo'lgan ta'siri uning oqibatlari va shu muammoni hal qilish yo'llari haqida fikr yuritamiz.*

Kalit so'zlar: *kiberjinoyat, muammo, iqtisodiyot, noqonuniy, viruslar, sypware, raqamlashtirish, dasturlar, ransomware, axborot, zararlar, hukumat.*

Hozirgi kunda yoshlarning ko'pchiligi onlayn muhitga to'g'ridan-to'g'ri smartfon va boshqa qurilmalar orqali bog'lanishmoqda va moslashib ham bo'lishdi, shu sababli har xil chetdan ularga bo'lgan ta'sirlar ham anchagina ko'paydi desak mubolag'a bo'lmaydi. Bu natijasida, kiberjinoyat ham kelajak avlod yoshlarning ichida jadal ko'paydi va ularning Internet tarmoq orqali jinoyati kundan-kunga oshmoqda. Bu muammoni dolzarbligi shundaki bizning yoshlar kiberjinoyat va kiberhujumni nima ekanligi hali to'la anglashgani yo'q yani asosiy muammo oqibatda ularni kelajagi barbod bo'lishidir va davlat iqtisodiyotini qulashi bilan bog'liqdir.

"Yoshlar texnologiyaga bo'lgan qiziqishlari va tajribasizliklari sababli kiberjinoyatlarga jalb etilish xavfiga duch keladi. Bu holat ularga yetarli darajada raqamli savodxonlik va axloqiy ko'nikmalar berilmaganida kuchayadi."[1]

Kiberjinoyat - bu kompyuter tarmoqlari, internet yoki boshqa texnologik vositalar yordamida sodir etiladigan huquqbuzarliklarning umumiy nomi.

Ushbu jinoyat turlariga noqonuniy ma'lumot olish, shaxsiy yoki tijorat ma'lumotlarini o'g'irlash, moliyaviy firibgarlik va boshqa turli xil huquqbuzarliklar kiradi. Kiberjinoyatlar odatda moliyaviy foyda olish yoki ma'lumotlarni buzish,

tarqatish, noqonuniy foydalanish maqsadida amalga oshiriladi.

Kiberjinoyatlar o‘zining ko‘lami va xilma-xilligi bilan ajralib turadi. Quyida uning asosiy sohalari haqida to‘xtalib o‘tamiz: Moliyaviy firibgarlik bu kiberjinoyatning eng keng tarqalgan turi bo‘lib, odatda bank kartalaridan noqonuniy foydalanish, onlayn savdo platformalaridagi firibgarliklar yoki soxta veb-saytlar yaratish orqali amalga oshiriladi.

Bunday jinoyatlar nafaqat jismoniy shaxslarga, balki bank va moliyaviy tashkilotlarga ham katta zarar yetkazadi.

Shaxsiy ma’lumotlarni o‘g‘irlash deganda kiberjinoyatchilar odamlarning shaxsiy ma’lumotlarini noqonuniy yo‘l bilan qo‘lga kiritib, ularni shantaj qilish, firibgarlik yoki boshqa noqonuniy maqsadlarda ishlatishi mumkin. Bu turdagi jinoyatlar identifikatsiya o‘g‘irligi deb ham ataladi.

Kiberjinoyatlarning yana bir jiddiy sohasi bu kiberterrorizmdir. Bunda jinoyatchilar davlat tizimlariga yoki strategik ob’ektlarga hujum qilib, ularni izdan chiqarish va xavfsizlikka tahdid solish maqsadini ko‘zlaydi. Bu turdagi jinoyatlar nafaqat davlatga, balki xalqaro hamjamiyatga ham xavf tug‘diradi. Noqonuniy dasturlar tarqatish esa kiberjinoyatchilar odatda zararli dasturlar (viruslar, troyanlar, spyware) orqali foydalanuvchilarning shaxsiy kompyuterlari yoki korporativ tizimlariga kirib, ma’lumotlarni yo‘q qilish yoki o‘g‘irlashga urinishadi.

Kiberpornografiya va shunga o‘xshash noqonuniy turdagi kontentlar tarqatish yoki ulashish jinoyatlarda jinoyatchilar internet orqali noqonuniy kontent, jumladan bolalar pornografiyasini tarqatadilar. Bu esa butun dunyo miqyosida keskin tanqid va qarshilikka duch kelmoqda. Shu kabi kiberjinoyatlar hozirgi raqamli davrda juda ham ko‘plab odamlarning mulkiga va ayniqsa fuqorolarning Konstitutsiyaviy huquq va erkinliklariga zarar yetkazish bilan yakunlanyapti.

Bundan tashqari, shu kabi jinoyat turlari agar shu asnoda ortib borishsa davlatning ham moliyaviy farovonligiga rahna solishi muqarrardir, chunki kiberhujumga uchragan fuqorolar aksariyat o‘z mablag‘larini yo‘qotishadi keyin esa ular ehtimol soliq va boshqa davlat tomonidan qat’iy belgilangan to‘lovlarni o‘z vaqtida amalga oshira olmasligi mumkin. Qo‘shimchasiga, mamlakatda o‘rnatilgan fuqorolik jamiyati ravnaq topa olmasligi shubhadan holi emas.

Malumki, butun dunyo raqamlashtirish jarayonida islohotlar qilayotgan paytda O‘zbekiston Respublikasi ham yuqori islohotlar olib bormoqda ulardan “O‘zbekiston Respublikasining 2030 strategiyasida raqamli iqtisodiyotning rivojlanishi muhim o‘rin tutadi.

Mamlakatda raqamli iqtisodiyotni faol rivojlantirish va axborot-kommunikatsiya texnologiyalarini keng joriy etish bo‘yicha bir qator chora-tadbirlar amalga oshirilmoqda.

Ushbu tadbirlar orasida elektron hukumat tizimini takomillashtirish, dasturiy mahsulotlar va axborot texnologiyalarining mahalliy bozorini rivojlantirish, shuningdek, ITparklarni tashkil etish kabi loyihalar mavjud.” [2] Shu kabi loyihalar ilgari surildi va bu mamlakat yosh avlodini kiberjinoyatga bo‘lgan tushunchasini

o‘zgartirish ko‘zda tutilgan. Ammo kiberjinoyatda shu kungacha bir qancha noqonuniy ishlar sodir bo‘lgan shuning uchun biz quyidagi ma’lumotlarga to‘xtalib o‘tamiz.

Tahminlarga ko‘ra, 2024-yilda kiberjinoyatchilikning global qiymati 9,5 trillion dollarga yetadi. Bu raqamni anglash uchun oddiy bir faktga e’tibor berish kerak: kiberjinoyatchilik ko‘plab mamlakatlarning yalpi ichki mahsulotidan (YaIM) oshib ketadi. Hatto dunyoning eng yirik iqtisodiyotlari ham kiberjinoyatlardan keltirilgan zararni jilovlashda qiyinchilikka duch kelmoqda. Bundan ham achinarlisi, 2025-yilga kelib, bu zarar har yili 10,5 trillion dollarga yetishi kutilmoqda. Tasavvur qiling, bu raqam yildan-yilga o‘sishda davom etayotgan, kiberjinoyatchilikni o‘ziga xos “soya iqtisodiyoti”ga aylantiradi.

Bundan tashqari, ransomware ya’ni to‘lov dasturlari orqali amalga oshiriladigan hujumlar, bugungi kunda eng xavfli kiberjinoyatlardan biri hisoblanadi.

2024-yilda ransomware tashkilotlarga 42 milliard dollarlik zarar yetkazishi ma’lumotlar qayd etilyapti. Ekspertlar 2031-yilga borib, ransomware tahdidlarining umumiy qiymati 265 milliard dollarga yetishini prognoz qilmoqda. Yanada dahshatli statistikani keltirsak: o‘sha yilga kelib, har ikki soniyada bitta ransomware hujumi sodir bo‘ladi.

Bu raqamlar oddiy statistik ko‘rsatkichlar emas, ular muayyan tashkilotlarning hayotiga, obro‘siga va moliyaviy barqarorligiga to‘g‘ridan-to‘g‘ri tahdid qilishini anglatadi. Bugungi kunda ransomware o‘zining chastotasi va murakkabligi bilan ajralib turadi, shu sababli har bir tashkilot o‘z himoya choralarini qayta ko‘rib chiqishi lozim.

Ma’lumotlar buzilishi ham kiberjinoyatchilikning yana bir jiddiy oqibatidir. 2023-yilda dunyo bo‘ylab ma’lumotlar buzilishidan o‘rtacha global zarar 4,45 million dollarni tashkil etdi. Bu uch yil ichida 15% o‘sish degani. Albatta, bu oddiy ko‘rsatkich emas; bunday hujumlar faqat kompaniyalarga moliyaviy zarar yetkazib qolmay, mijozlar ishonchini ham yemiradi.

Sog‘liqni saqlash, hukumat va infratuzilma kabi sohalar ayniqsa yuqori xavf ostida. Bu sohalar nafaqat qimmatli ma’lumotlarga ega, balki ularning buzilishi ijtimoiy ahvolga ham katta ta’sir ko‘rsatishi mumkin. Masalan, sog‘liqni saqlash tizimidagi hujumlar bemorlarning hayotini xavf ostiga qo‘yadi yoki davlat infratuzilmasiga zarar yetkazish butun mamlakatni falaj qilishi mumkin.

Kiberjinoyatchilik oddiy texnologik muammo emas, balki butun dunyo uchun dolzarb tahdidga aylanib bormoqda. Uning hajmi, murakkabligi oshib borayotgani faqat kompaniyalar emas, davlatlarni ham bu masalani jiddiy ko‘rib chiqishga undaydi. Innovatsiyalar rivojlanayotgan bir vaqtda kiberxavfsizlik masalalarini chetlab o‘tib bo‘lmaydi. Shunday ekan, kiberjinoyatchilarning oldini olish uchun kuchli tizimlar, puxta strategiyalar va global hamkorlik zarur. Aks holda, tahdidlar yanada kuchayib, yoshlar uchun yomon oqibatlarga olib kelishi aniq.

O‘smirlar shu yuqorida keltirilgan ma’lumotlarni o‘rganishi uchun O‘zbekiston Respublikasi 2030 startegiyasi va boshqa omillar sabab bo‘ladi.

Ularning ertangi hayoti shu kabi kiberjinoyatlardan holi bo‘lishi uchun bir qancha islohotlar taklif hamda bajarilish muhimdir.

Birinchidan, ҳуқуқий ta’lim va xabardorlikni oshirish.Kiberjinoyatlar xavflari haqida yoshlarni xabardor qilish juda muhimdir. Maktablarda va oliy ta’lim muassasalarida raqamli xavfsizlik bo‘yicha maxsus kurslar tashkil etish zarur.

Yoshlar internetda xavfsiz harakat qilishni o‘rganishlari, shaxsiy ma’lumotlarini qanday himoya qilishni bilishlari kerak. Shu bilan birga, onlayn ta’qiblarni oldini olish bo‘yicha pedagoglar va psixologlar tomonidan maslahatlar berilishi lozim.

Yoshlar o‘zlarini onlayn muhitda qanday himoya qilishlarini tushunishlari uchun raqamli xavfsizlik bo‘yicha treninglar o‘tkazilishi kerak. Bu jarayon, nafaqat yoshlarni himoya qilishga, balki ularni kiberjinoyatlarning oldini olishga va internetda ehtiyotkorlikni oshirishga qaratilgan bo‘lishi kerak. Ta’lim tizimi yoshlarni nafaqat zamonaviy texnologiyalarni o‘rganishga, balki ularni xavfsiz va mas’uliyatli ishlatishga o‘rgatishi lozim.

Ikkinchidan, axborot texnologiyalari bo‘yicha mutaxasislarni tayyorlash. Bu mutaxassislar kiberjinoyatlarga qarshi samarali kurashish va raqamli jinoyatchilikni kamaytirish uchun zarur vositalarni yaratishi mumkin. Yoshlarni kiberxavfsizlik bo‘yicha amaliy treninglar va kurslar bilan ta’minlash, ularga xavfsizlikni ta’minlashda qanday texnik vositalardan foydalanish, qanday huquqiy me’yorlar borligini o‘rgatish kerak.

O‘zbekiston kabi rivojlanayotgan mamlakatlar uchun axborot xavfsizligi bo‘yicha kadrlarni tayyorlash, uzoq muddatli strategik maqsadlardir. Shu tariqa, yoshlar kiberjinoyatlarga qarshi kurashishda faollik ko‘rsatishi, bu sohada o‘z bilimlarini amalda qo‘llay olishlari muhim.

Yoshlarni raqamli tarmoqlarda xavfsiz foydalanish choralarini yaratish deganda kiberjinoyatlarni oldini olish uchun yoshlar va ota-onalar, o‘qituvchilar o‘rtasida yaqindan hamkorlik qilish zarur.

Ota-onalar o‘z farzandlariga internetda xavfsiz qolish uchun qadam-baqadam ko‘rsatmalar berishlari, internetda ehtiyotkorlikni o‘rgatishlari kerak.

Yoshlar o‘zlarini kiberjinoyatlardan himoya qilishda qanday choralar ko‘rishlarini bilishlari lozim.Internetda ma’lumotlarni shifrlash, shaxsiy ma’lumotlarni oshkor qilmaslik kabi oddiy, ammo samarali amallarni amalga oshirish kerakligini tushuntirish lozim.

Yangi texnologiyalarni joriy etish, raqamli jinoyatchilikka qarshi tizimli choralar ko‘rish uchun maxsus texnik vositalar yaratish lozim. Kiberjinoyatlarni aniqlash va jinoyatchilarni jazolash tizimini takomillashtirish, qonunlarni yangi raqamli haqiqatga moslashtirish juda muhimdir.

Buning uchun davlat darajasida maxsus huquqiy normativlar va yuridik mexanizmlar ishlab chiqilishi lozim. Kiberxavfsizlik bo‘yicha Hukumat tashabbuslari kiberxavfsizlikka alohida e’tibor qaratish, raqamli jinoyatlarni kamaytirish va yoshlar orasida axborot xavfsizligini oshirish uchun hukumat tomonidan aniq chora-tadbirlar ishlab chiqilishi kerak. Kiberxavfsizlik bo‘yicha

qonunlar va me’yorlarni takomillashtirish, xalqaro hamkorlikni rivojlantirish, va texnologik infratuzilmani mustahkamlash orqali yoshlarni kiberjinoyatlardan himoya qilishda muhim qadamlar tashlash muhimdir. Hukumatning tashabbuslari yoshlar uchun raqamli xavfsizlikni ta’minlashda mustahkam asos bo‘lishi kerak.

Bundan tashqari, O‘zbekiston Respublikasi bir qator qonunlar va normativhuquqiy hujjat chiqargan va unda kiberjinoyanti to‘xtatish va uni yoshlarga ta’sirini oldini olish maqsadida “kiberxavfsizlik” choralarini ko‘rgan, ya’n “Kiberxavfsizlik – bu kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati.” [3]

Xulosa qilib aytganda, kiberjinoyatlar bugungi kunda yoshlar tarbiyasiga jiddiy tahdid tug‘dirmoqda. Internetning keng tarqalishi va texnologiyalarning rivoji natijasida yoshlar noqonuniy faoliyatlarga duch kelmoqda yoki o‘zlari ham bilmasdan ularga aralashib qolmoqda. Bu esa nafaqat yoshlarning kelajagiga, balki jamiyatning iqtisodiy va ijtimoiy barqarorligiga salbiy ta’sir ko‘rsatadi.

FOYDALANILGAN ADABIYOTLAR

1. Jason Brown, “Youth and Cybercrime: A Growing Concern,” 2015. - AQSH.
2. O‘zbekiston Respublikasi Prezidentining Farmoni, 11.09.2023 yildagi PF-158-son Toshkent, www.lex.uz
3. O‘zbekiston Respublikasining Qonuni, 15.04.2022 yildagi O‘RQ-764-son. - Toshkent, www.lex.uz

GLOBALLASHUV DAVRIDA KIBERJINOYATLARNI SODIR ETILISHIDAGI MUAMMOLAR

Hakimboyeva Dildora Ma’rufjon qizi
Ilmiy rahbar: yu.f.d.(PhD) I.Atamirzayev

Namangan davlat universtiteti Yuridik fakulteti 1-bosqich talabasi

Annotatsiya. Ushbu maqolada kiberjinoyat nima ekanligi, uning paydo bo‘lish sabab hamda oqibatlari haqida ma’lumotlar beriladi. Shu bilan birgalikda uni oldini olish uchun ayrim mulohazalar ham keltirib o‘tiladi.

Kalit so‘zlar: Kiberxavfsizlik markazi, axborot xavfsizligi, kompyuter viruslari, kiberjinoyat, yangi texnologiyalar , normativ hujjatlar, kiberxavsizlik.

Bugungi globallashuv davrida ommaviy axborot vositalari juda ham rivojlanmoqda.Inson xohlagan ma’lumotlarini internet saytlari orqali hech qanday qiyinchiliklarsiz olish imkoniyatiga ega.Jahonda to‘qqiz milliarddan oshiq inson bor bo‘lsa ular olayotgan ma’lumotlar undan ham ko‘p hisoblanadi.Ammo odamlarga borayotgan bu ma’lumotlar qanchalik to‘g‘ri yoki no‘tog‘riligiga ham e’tibor berish kerak. Bundan tashqari internet saytlarida berilayotgan ma’lumotlardan ba’zilar xolis niyatda foydalanadi, ba’zilar esa yomon niyatda.Shuning uchun ham bugungi kunda

axborotlarni olish , ularni tarqatish qanchalik global bo‘layotgan bo‘lsa uni himoya qilish , turli ma’lumotlar ta’siriga qarshi kurashish ham dolzarb masala hisoblanadi.

Hozirgi davrga kelib jahonning barcha mamlaktlarida axborot xavfsizligini ta’minlash eng muhim masalalardan biri sanaladi.Chunki axborot texnologiyalari orqali insonlar turli xil katta-kichik jinoyatlar qilishmoqda.Bu jinoyatlardan biri esa kiberjinoyatdir.

Dunyoda jinoyatlarning juda ham ko‘p turlari mavjud va ulardan biri kiberjinoyatdir.U jahonda eng ko‘p sodir etilayotgan jinoyatlar orasida to‘rtinchi o‘rinda turadi. O‘zgalar mol-mulkini internet yoki kompyuter vositalari orqali talon-taroj qilish jahonda shiddat bilan o‘sib borayotgan va chegara bilmaydigan jinoyat ekani bilan xavflidir.

Kiberjinoyat – bu boylik orttirish yoki boshqa g‘arazli niyatlarda axborot texnologiyalardan noqonuniy tarzda foydalanib sodir etilgan jinoyat hisoblanadi. Uning asosiy turlari viruslar yordamida zarar yetkazuvchi dasturlarni tarqatish, parollarni buzib kirish, kredit karta va boshqa bank rekvizitlaridagi raqamlarni o‘g‘irlash, shuningdek, internet orqali qonunga zid axborotlarni tarqatish kabilar kiradi.

Viruslar orqali zarar yetkazishda “ kompyuter viruslari egasini ogohlantirmay va uning istagiga qarshi uning dasturiga „joylashtiriladi“ va zaryadlangan faylni navbatdagi qo‘yishda ko‘payadi. Kompyuter virusi kompyuterning risoladagi ish me’yorini buzadi, ma’lumotlarni o‘chirib yuboradi, displey (monitor) ekranidagi tasvirni buzadi, hisoblash jarayonini sekinlashtiradi.”[60]

Parollarni buzib kirish- bu insonlarni shaxsiy ma’lumotlarini bilib undan noqonuniy yo‘lda foydalanish uchun axborot tizimini buzib kirish hisoblanadi.Bu ham eng keng tarqalgan kiberjinoyat turlaridan biridir.

Kredit karta va bank rekvizitlardagi raqamlarni o‘g‘irlash-bu juda ko‘p mamlakatlarda kuzatiladigan jinoyat hisoblanadi. Bunda jinoyatchilar odatda katta bank hisob raqamiga noqonuniy usul bilan kirib pullarni yechib olishadi.

Kiberjinoyatning kelib chiqishi sabablari global internet yaratilishi bilan bog‘liqdir.Ya’ni bu jinoyat turini insonlar minglab kilometr uzoqlikda joylashgan boshqa mamlakat tashkilotlarining bank hisob raqamiga axborot texnologiyalari orqali kirib mablag‘larini yechib olish orqali sodir etishmoqda.Shu kabi jnoyatlarni kim, qanday qilmoqda degan savollar ba’zi hollarda javobsiz qolib ketyapti. Misol uchun , Rossiya Federatsiyasi axborot agentliklari ma’lumotlariga ko‘ra 2015 -yilning o‘zida ushbu davlatda kiberjinoyatchilikka oid o‘ttiz mingga yaqin huquqbuzarliklar sodir etilgan.Bu kabi qonunbuzarlklar zamirida moddiy manfaat yotgani hech shubhasizdir. Negaki, kiberjinoyatning tag zamirida moddiy manfaatga erishish turadi.

Albatta, O‘zbekiston ham kundan kunga yangilanib , har soha bo‘yicha rivojlanib bormoqda.Yangidan yangi texnologiyalar ishlab chiqarilmoqda, yurtimizdagi ko ‘p sonli aholi deyarli barcha ma’lumotlarni gadjetlardan olishmoqda.Shuning uchun ham yurtimizda axborotlarni jinoyatlardan himoya qilish maqsadida turli normativ hujjatlar qabul qilingan.

[60] https://taqdimot1.wordpress.com/2019/02/01/viruslar/

Xususan, O‘zbekiston Respublikasi Konstitutsiyasining 31-moddasida: “Har kim yozishmalari, telefon orqali so‘zlashuvlari, pochta, elektron va boshqa xabarlarni sir saqlanishi huquqiga ega.Ushbu huquqning cheklanishi faqat qonunga muvofiq va sudning qarori asosan yo‘l qo‘yiladi”[61] ,- deb belgilab qo‘yilgan.

Бugungi zamonda g‘arazli niyatlarda insonlar boshqalarning shaxsiy ma’lumotlariga kirib ularni tarqataman deb tahdid qilib insonlardan pul talab qilishmoqda.Bunday qilmishlar nafaqat kiberjinoyatga , balkim boshqa salbiy oqibatlarga olib keladi, hattoki, bunday holatlarning oxiri inson hayotining yakunlanishi bilan ham tugashi mumkin.

Shu kabi oqibatlarni oldini olish uchun O‘zbekiston Respublikasida Kiberxavfsizlik markazi tashkil etilgan.Uning asosiy maqsadi kiberjinoyatga oid jinoyatlarni aniqlash, ularga qarshi kurashish, kiberjinoyatlarni oldini olish, kiberxavsizlikni ta’minlash hioblanadi.Kiberjinoyatdan zarar ko‘rgan fuqarolar markazga murojaat qiladilar.

O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash maqsadida “Kiberxavfsizlik to‘g‘risida” gi Qonun ishlab chiqildi.

Uning asosiy maqsadi raqamli texnologiyalar orqali sodir etiladigan jinoyatlarni tartibga solish va u borada qanday ishlarni amalga oshirish kerakligi belgilab qo‘yilgan.

Ushbu Qonunda kiberxavfsizlikka quyidagicha ta’rif beriladi: “**kiberxavfsizlik** — kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati”[1]

O‘zbekiston Respublikasi Prezidentining “O‘zbekiston – 2030” strategiyasi to‘g‘risidagi farmoni chiqarildi. Ushbu farmonda O‘zbekiston Respublikasida 2030-yilgacha amalga oshirilishi kerak bo‘lgan maqsadlar belgilab qo‘yilgan va bu farmon bo‘yicha tegishli davlat organlari , mansabdor shaxslar tomonidan bajarilishi kerak bo‘lgan vazifalar ko‘rsatib o‘tilgan. Shu bilan birgalikda bu farmonda kiberxavsizlikni ta’minlash, axborot savodxonligini oshirishga doir vazifalar ham keltirib o‘tilgan. Ularga quyidagilarni misol qilib keltirishimiz mumkin:

“Maktabgacha ta’lim tizimini yangi bosqichga olib chiqish hamda bolalarning to‘liq qamrovini ta’minlash maqsadida davlat maktabgacha ta’lim tashkilotlarini 100 foiz kompyuter sinfi bilan ta’minlash orqali tarbiyalanuvchilarda boshlang‘ich kompyuter savodxonligi ko‘nikmalarini shakllantirish va professional ta’lim tizimini rivojlantirish orqali o‘quvchilarni zamonaviy bilim va ko‘nikmalarga o‘rgatish maqsadida o‘rta bo‘g‘in mutaxassislarini tayyorlashda davlat grantini axborot texnologiyalari, qurilish, transport va logistika yo‘nalishlarida 100 foizga yetkazish.”[2]

Kiberjinoyatlarni oldini olish uchun qilinishi kerak bo‘lgan eng katta qadam bu yurtimizda IT sohasini yanada rivojlantirish va yosh avlodni raqamli texnologiyalardan to‘g‘ri, oqilona yo‘lda foydalanish ko‘nikmalarini hosil qilishdir.Shuni aytib o‘tish joizki, kiberjinoyatlarni oldini olish uchun yosh avlodga faqat IT ni o‘rgatish bilan cheklanib qolish noto‘g‘ri bo‘ladi.Negaki ular bu sohani o‘rganib g‘arazli niyatlarda foydalanishlari mumkin buni oldini olish maqsadida ularga kiberjinoyatlar qanday salbiy oqibatlarga olib kelishi haqida ham tushunchalar berishimiz zarur.Zero, ular

[61] https://lex.uz/docs/-6445145?otherlang=1

shundagina axborot tizimlaridan, raqamli texnologiyalardan oqilona, qonuniy foydalalanadilar va yurtimizda bu sohaga oid jinoyatlar kamayadi deb o‘ylayman.

FOYDALANILGAN ADABIYOTLAR

1.‘‘Kiberxavfsizlik to‘g‘risida” gi O‘zbekiston Respublikasining Qonuni, 15.04.2022 yildagi O‘RQ-764-son. Kuchga kirish sanasi 17.07.2022. (Qonunchilik ma’lumotlari milliy bazasi, 16.04.2022-y., 03/22/764/0313-son).
2. “ “O‘zbekiston — 2030” strategiyasi to‘g‘risida” O‘zbekiston Respublikasi Prezidentining Farmoni, 11.09.2023 yildagi PF-158-son. (1-ilova O‘zbekiston Respublikasi Prezidentining 2023-yil 25-dekabrdagi PF-214-sonli Farmoni tahririda - Qonunchilik ma’lumotlari milliy bazasi, 29.12.2023-y., 06/23/214/0984-son.
3. O‘zbekiston Respublikasi Konstitutsiyasi . 2023-yil 30-aprel.

CYBERCRIME IN THE MODERN ERA: UNDERSTANDING VISHING (VOICE PHISHING)

Academy MIA Qahorov Davronbek Rustambek o‘g‘li
MIA OSD center Cybersecurity MuhammadBobur Sodikov

In today’s interconnected world, the rise of cybercrime poses a persistent threat to individuals and organizations alike. Among the many forms of cybercrime, vishing, or voice phishing, has emerged as a potent method for exploiting human vulnerabilities. Leveraging the trust people place in verbal communication, cybercriminals manipulate victims into divulging sensitive information or making financial transactions. As technology advances, the tactics of these criminals evolve, making it imperative to understand and counteract vishing.

What is the definition of vishing?

Vishing, short for voice phishing, refers to fraudulent phone calls or voice messages designed to trick victims into providing sensitive information, like login credentials, credit card numbers, or bank details. These details can then be exploited for criminal activities such as fraud, identity theft, or financial theft. Phishing attacks are common and costly: In 2022, phishing was the second most-common cause of data breaches, costing organizations an average of US$4.91 million in breach expenses. In vishing scams, attackers pretend to be from reputable organizations (such as the victim's bank, the IRS, or a package delivery service) and make unexpected phone calls. They might use toll-free numbers or use voice over internet protocol (VoIP) technology to appear as trusted organizations.

What's the difference between vishing, phishing, and smishing?

Vishing, phishing, and smishing employ different types of communication, but their objectives are the same: taking control of accounts, committing fraud, or stealing funds from unsuspecting individuals or businesses.

Here is the difference between these three phishing methods:

Vishing: Phone call scams that pressure victims to share sensitive information verbally

Phishing: Email scams that lure victims into clicking links leading to deceptive websites or malware downloads

Smishing: Text message scams that also prompt victims to click malicious links or visit fake websites.

Advances in technology have evolved common vishing scams into incredibly convincing attacks. Capitalizing on human trust and urgency, these scams mimic real businesses and scenarios, resulting in serious consequences for organizations. Here are a few examples of common vishing attacks:

Social Security or Medicare scams. Older adults are often targets for cybercriminals as they may be less familiar with modern phishing scam tactics. In these scams, criminals pose as Social Security or Medicare officials to extract sensitive account details, allegedly to issue a new Social Security number or discuss benefits. The older adult demographic tends to favor phone communication over email or text messages, exposing themselves more to vishing schemes than to phishing or smishing attacks. Inform friends or family members whom you think are susceptible to these types of scams that the IRS, Social Security Administration, or Medicare will never call them demanding personal information or issuing threats. Legitimate federal agencies do not contact citizens by phone, email, text, or social media to request personal or financial information.

Voice-cloning vishing scams. Voice-cloning technology uses artificial intelligence to craft alarmingly realistic fake audio or video clips. Cybercriminals are now using these AI tools to fabricate voice recordings that mimic those of a target's family member or trusted figure. For instance, a CEO's voice can be replicated to request a significant financial transfer. A lower-ranking employee might believe the call is genuine due to the accurate voice imitation and comply due to a sense of urgency and respect for the authoritative request. As voice-cloning tools become more sophisticated and available, the risk of such scams grows, underscoring the need for strong security protocols and heightened vigilance—even when the caller sounds familiar.

Bank-impersonation scams. Bank-impersonation scams involve scammers impersonating credit card companies, banks, and other financial institutions to gain unauthorized access to your accounts. Claiming there is unusual or suspicious activity, they ask you to verify your account details and login credentials under the guise of resolving the issue. If you call your financial institution directly, you may be asked to verify your identity with confidential information. However, legitimate financial institutions will never call you to ask for your passwords or security code.

What should you do if you've experienced a vishing attack?

If you've fallen victim to a vishing attack, taking immediate steps can help mitigate potential harm and prevent further exploitation of your information. Here is what you can do:

- Alert your financial institutions of the fraudulent activity, and request to freeze or monitor your accounts for unusual activities.
- Change all compromised passwords, PINs, and security credentials on your accounts, using unique, strong passwords for each.
- Notify the relevant company or institution that the scammer claimed to represent, as they may provide additional assistance and take steps to warn others.

- If you're an employee who disclosed sensitive corporate information, immediately inform your company's IT department or cybersecurity team to initiate damage control protocols.

Vishing and other cybercrimes will continue to exploit the public for as long as scammers can successfully deceive individuals. However, taking the time to identify and counter vishing attempts can help diminish their effectiveness. Keep reading to learn how you can prevent vishing attacks.

In conclusion, vishing, or voice phishing, is a deceptive cybercrime tactic where attackers use phone calls to trick individuals into revealing personal, financial, or sensitive information. Unlike phishing, which primarily occurs through emails, and smishing, which leverages text messages, vishing manipulates the trust people associate with verbal communication to exploit their vulnerabilities.

Understanding the distinctions between these forms of social engineering is crucial for protecting oneself. Phishing relies on fraudulent emails to mislead victims, while smishing uses misleading text messages. Vishing, however, adds a layer of psychological pressure by engaging directly with the victim via phone, making it feel more immediate and legitimate.

If you have experienced a vishing attack, swift action is essential. Report the incident to your bank, credit card provider, or any other institution that may be affected. Change passwords or security credentials tied to your accounts, and monitor your financial statements for unauthorized transactions. Additionally, report the attack to the appropriate authorities or cybersecurity organizations to help track and mitigate similar threats.

By staying informed, vigilant, and proactive, individuals and organizations can reduce the risk of falling victim to vishing and other cyber threats. Remember: when it comes to safeguarding your information, caution is always your strongest defense.

LEGAL, ORGANIZATIONAL, FINANCIAL-ECONOMIC, AND TECHNICAL CHALLENGES AND SOLUTIONS IN COMBATING CYBERCRIME: THE CASE OF BANK CARD CLONING

Academy of the MIA Behruzjon Bozorov
MIA OSD center Cybersecurity Jamshid Erkinov

Annotation. This article explores the critical issue of combating cybercrime with a specific focus on bank card cloning. It examines the legal, organizational, financial-economic, and technical challenges that arise in addressing this prevalent form of cybercrime. The study highlights the importance of robust legal frameworks, enhanced organizational measures, and cutting-edge technological solutions to mitigate the risks associated with card cloning. Furthermore, it discusses the economic implications of such crimes on financial institutions and individuals. By analyzing international best practices and proposing comprehensive solutions, the article aims to contribute to the development of more effective strategies in combating cybercrime, particularly in the financial sector.

Keywords: Cybercrime, bank card cloning, cybersecurity, legal challenges, organizational strategies, financial implications, technical solutions, fraud prevention, digital security

Introduction

Cybercrime continues to evolve rapidly, posing significant threats to individuals, organizations, and national economies. Among the various forms of cybercrime, bank card cloning has emerged as one of the most pervasive and damaging activities. This illegal practice involves duplicating sensitive card information through skimming devices or hacking methods, leading to unauthorized transactions and financial losses. The global financial sector faces increasing pressure to address these threats and protect the integrity of its systems.

This article delves into the multidimensional aspects of combating bank card cloning. It begins by exploring the legal frameworks governing cybercrime, emphasizing the need for updated laws that specifically address emerging digital threats. The study then examines organizational measures, including the role of financial institutions and regulatory bodies in preventing and mitigating fraud. Additionally, it highlights the financial-economic impact of card cloning on stakeholders and the broader economy, outlining the costs associated with fraud detection, resolution, and consumer trust rebuilding.

A significant portion of the article is dedicated to technical solutions, showcasing how advancements in cybersecurity technology, such as artificial intelligence, encryption, and real-time monitoring, can be leveraged to combat cloning activities effectively. Finally, the article proposes a comprehensive, interdisciplinary approach that integrates legal, organizational, financial, and technical measures to tackle this pressing issue.

Through an analysis of current challenges and potential solutions, this study aims to provide actionable insights and recommendations for policymakers, financial institutions, and cybersecurity professionals striving to safeguard the financial ecosystem from cybercriminals.

Legal Challenges and Solutions

The fight against bank card cloning begins with the establishment of robust legal frameworks. Many countries lack specific legislation to address the unique nature of cybercrime, leading to gaps in prosecution and enforcement. Harmonizing national laws with international conventions, such as the Budapest Convention on Cybercrime, is essential for enhancing global cooperation. Effective laws should also impose stringent penalties to deter offenders and provide clear guidelines for handling digital evidence.

Organizational Strategies

Financial institutions play a pivotal role in combating bank card cloning. Implementing strict operational policies, such as multi-factor authentication (MFA) and customer verification protocols, can significantly reduce cloning risks. Training employees and raising customer awareness about phishing and skimming techniques are equally crucial. Collaboration between banks, regulators, and cybersecurity firms fosters a unified defense strategy.

Financial-Economic Implications

Bank card cloning results in substantial financial losses for institutions and consumers alike. Banks must allocate significant resources to fraud detection and compensation, which can erode profit margins. Additionally, the reputational damage caused by such incidents can reduce customer trust. To mitigate these impacts, financial institutions should invest in advanced fraud detection systems and insurance mechanisms to offset potential liabilities.

Technical Solutions

Technological advancements offer promising tools for combating card cloning. Solutions such as chip-based EMV (Europay, MasterCard, Visa) technology have proven effective in reducing fraud associated with magnetic stripe cards. Artificial intelligence (AI) and machine learning (ML) algorithms can analyze transaction patterns to identify and flag suspicious activities in real-time. Biometric authentication methods, including fingerprint or facial recognition, add an additional layer of security.

Integrated Approach

An interdisciplinary approach that combines legal, organizational, financial, and technical measures is necessary to combat bank card cloning effectively. Policymakers should work closely with financial institutions and technology providers to design holistic strategies that address this multifaceted issue.

Conclusion

Bank card cloning remains a significant threat in the digital era, with far-reaching legal, financial, and technical implications. This article has outlined the challenges and solutions in tackling this issue through robust legal frameworks, organizational policies, economic strategies, and technological advancements. By adopting an integrated approach, stakeholders can enhance their defenses against cybercriminals and safeguard the financial ecosystem. Addressing these challenges requires collective action from governments, financial institutions, and technology experts. Future efforts must focus on fostering innovation, improving international collaboration, and enhancing public awareness to reduce the prevalence of card cloning and its impact on society.

References

1. Budapest Convention on Cybercrime, Council of Europe.
2. Europay, MasterCard, Visa (EMV) Standards, EMVCo.
3. Smith, J. (2021). *The Economics of Cybersecurity*. Financial Times Press.
4. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
5. Cybersecurity and Infrastructure Security Agency (CISA). (2022). *Guidelines for Payment Card Security*.
6. International Telecommunications Union (ITU). (2023). *Global Cybersecurity Index Report*.
7. Singh, R. (2021). "The Role of AI in Fraud Detection," *Journal of Financial Technology*.

Bank for International Settlements (BIS). (2022). *Cyber Resilience in Financial Systems*.

КИБЕР ЖИНОЯТЧИЛИКДА ТАҲДИД ВА ҲИМОЯ

Баҳромжон Бахтиёрович Турғунбаев

Ўзбекистон Республикаси, ИИВ Малака ошириш институти, Касбий тайёргарлик факультети, Махсус фанлар цикли ўқитувчиси
тел; +99899-833-35-57

Отаев Ўткирбек Матёқубович

Ўзбекистон Республикаси ИИВ Малака ошириш институти Касбий тайёргарлик факультети Махсус фанлар цикли катта ўқитувчиси
Тел:+99897 775 08 83
E-mail: otayev1983@mail.ru

Жамият шиддат билан тараққий этаётган бугунги кунда ҳар бир инсон ахборот технологияларининг имкониятларидан кенг фойдаланмоқда. Хатто молиявий хизматларни кўрсатишда ҳам интернет дўконларининг таклифи қулайлигини эътироф этадиганлар кўпчиликни ташкил этмоқда. Аммо сир эмас вертуаль оламда чув тушаётганлар ҳам оз эмас.

Шу мақсадга йўналтирилган тарғибот тадбири вилоят Ички ишлар бошқармаси Тезкор қидирув хизмати Киберхавфсизлик бўлими ҳамда алоқадор идоралар ходимлари билан ҳамкорликда ташкил этилди. Масъуллар томонидан таъкидланганидек, Мамлакатимизда 30 мингга яқин интернет фойдаланувчилари борлигини инобатга оладиган бўлсак, уларнинг орасида сиз-у биз ҳам бор, бу кўрсаткич кибер жиноятчилар учун каттагина даромад аудиторияси ҳисобланади.

Мулоқотларда ижтимоий тармоқлар интернет дўконлардан фойдаланишда белгиланган тартиб қоидаларга амал қилмаслик оқибатида фирибгарларнинг тузоғига тушиб қолиш ҳеч гап эмаслиги, пластик карта пинкоди ва паролини шунингдек смс хабарлар орқали юбориладиган махфий кодларни бегона шахсларга бермаслик кераклиги уқтирилши лозим.

Россия ҳудудида «Asacub» ҳамда «Svpeng» номли вируслар оиласи оммалашган. Бу вируслар жамланмаси маълум бир сайт эгаси Google сайтига реклама қўйишга рухсат бериши эвазига ундан пул олиши мумкин бўлган Google AdSense хизмати орқали тарқалган. Бунда Google рекламаси мавжуд сайтга кирган Android фойдаланувчиси зарарли файлни юқтириб олади ва хакерларнинг «қурбони»га айланади.

Шу боис, ахборот хавфсизлиги соҳаси мутахассислари Android операцион тизимида фаолият кўрсатувчи девайслар эгаларига интернетдан фойдаланишда ишончли манбааларга киришни маслаҳат бермоқдалар. Айниқса, банк-молиявий иловалари ўрнатилган мобиль қурилмаларга зарарли иловаларни ортириб олиш катта йўқотишларга сабаб бўлиши мумкин.

АҚШнинг Arbor Networks дастурий таъминот ишлаб чиқарувчи компанияси томонидан ўтказилган тадқиқот натижалари маълум қилишича, ишлаб чиқариш, компаниялар ўртасидаги рақобатнинг кучайиши уларни виртуал дунёда ҳам

рақибга айлантирган ва компаниялар рақибларининг онлайн савдоси ёки тизимларини ишдан чиқариш мақсадида, хакерларни ёлламоқдалар.

Замонавий кибержиноятчилик орқали бугун хакерлар уларни ёллаётган муассасаларга хизматларини сотишга муваффақ бўлмоқдалар. Улар ўзлари кирган тизимлардан маълумотларни ўғирлаб, мижозларига сотадилар. Ёки ёлланма қотиллар каби, бошқа компаниянинг ахборот тизимларини йўқ қиладилар.

Ушбу хизматлари учун хаккерларга соатига 2.50 АҚШ доллари миқдорида иш ҳақи тўланар экан. Айниқса, бир нечта компьютерлар тармоғида хизмат кўрсатишни рад қилувчи зарарли тизимларнинг ўрнатилиши, яъни DDoS-ҳужумларга эҳтиёж ортиб бормоқда.

Тахминан ҳар йили 15 млн нафар АҚШ фуқароларига, асосан компания раҳбарларига оид 50 млн АҚШ доллари миқдоридаги зарарга тенг бўлган шахсий маълумотлар интернет тармоғига уюштирилган ҳужумлар оқибатида ўғирланади. Таҳлиллар бу каби жиноятларнинг асосан дам олиш кунларида содир бўлишини кўрсатади.

Arbor Networks таҳлилчиси Деннис Шварцнинг маълум қилишича, хакерларнинг соатига 2-3 АҚШ доллари ишлашлари кутилмаган ҳолат. Боиси, ривожланган мамлакатларда хакерлик учун жиноятчилар қатъий жазога тортиладилар. Уларнинг арзимаган маблағ эвазига жиноятга қўл уришлари эса ачинарли.

Энг кўп кузатилаётган 3 кўринишдаги ахборот хуружлари қайд этилди.

Экспертларнинг фикрича, фишинг орқали маълумотларни ўғирлаш, махфий мақсадга эга мобиль иловалар орқали электрон қурилмаларга кириб бориш ва алоқанинг ҳимоя қилинмаган каналларини томоша қилиш орқали бугун кўпчилик интернет фойдаланувчилари кибер жиноятларнинг қурбонига айланмоқда.

Бугунги кунда кибер жиноятчиликда муайян шахснинг ёки объектнинг географик жойлашган нуқтаси тўғрисида хабар тарқатиш, шахсий маълумотлар базасини бузиб кириш каби хизматлар оммалашган. Хаккерлар бу каби маълумотларни интернет ва ижтимоий тармоқ фойдаланувчилари томонидан турли электрон ресурсларга уларнинг фойдаланиш шартларини ўқимасдан туриб киришлари эвазига олишмоқда.

Яъни, биз ижтимоий тармоқда дуч келадиган «Неча йил яшайсиз? «, «АҚШ президенти сиз ҳақингизда нима дейди? «, «Қайси Голливуд актёрига ўхшайсиз» каби хизматлар аслида фишинг бўлиб, сиз улардан фойдаланиш чоғида уларнинг шартига рози бўласиз ва ўзингиз тўғрингиздаги маълумотларни уларга ҳадя қилган бўласиз. Бу маълумотлар эса махфий равишда ташкил этилган йирик «қора ахборот бозорлари»да катта маблағга сотилади.

Ўзбекистондаги ҳолат «Касперский лабораторияси»нинг гувоҳлик беришича, Ўзбекистонда кибер хуружга учраётганларнинг 1,6 фоизига банк-троянлари зарар етказмоқда. Кибер-вирус хуружига учраганлар орасидан банк-троянларининг қурбонига айланган фойдаланувчилар улуши бўйича

Мобиль қурилмалар хавф-хатари географиясига мувофиқ, Ўзбекистондаги мобиль қурилмаларга йилида 1000 тадан 50 мингтагача зарарли вирусга эга иловалар зарар етказади.

Кучли пароллар ўрнатиш компьютер тизимларига киришга рухсат берувчи паролларни ҳар 6 ойда бир марта янгилаш зарурлигини жаҳонинг аксарият компаниялари одатларига айлантиришган. Аксарият хакерлар умумий пароллар билан ҳужум уюштирадилар.

Ходимларни ўқитиш зарур шуни алоҳида таъкидлаш жоизки, ходим – хавфсизликнинг энг нозик нуқтаси. Фишинг-ҳужумлар фойдаланувчининг электрон почтаси, ижтимоий тармоғидаги саҳифалари орқали ахборотларни ўғирлашга уринишади. Хакер логин ва махфий сўзларни аниқлашга уриниб, ходимларга сохта, аслига айнан ўхшаш сайтларнинг манзилини юборади. Бу кибер жиноятчиликнинг олдини олиш учун эса ходим малака ва билимга муҳтож.

Маълумотларни назорат қилиш махфий маълумотларнинг хакерлар қўлига тушиш ҳолати кўпроқ собиқ ходимлар билан боғланади. Шунингдек, заиф веб-сайтлар, айниқса онлайн тўлов ҳамда тизимлар ўрнатилган сайтларда кучли ҳимоялаш чораларини кўриш зарур.

Информацияни шифрлаш муҳим информация доимо шифрланган шаклда сақланиши лозим. Яъни, маълумотларни шифрлаш тизимларини ўрнатиш мақсадга мувофиқ.

Мутахассисларнинг фикрича, агар ҳар бир интернет фойдаланувчиси ва хизмат кўрсатувчилар кибер оламда ҳам ҳаётдаги каби эҳтиёткорликни унутмасалар, аксарият кибер жиноятларнинг олди олинган бўлар эди.

Жамият шиддат билан тараққий этаётган бугунги кунда ҳар бир инсон ахборот технологияларининг имкониятларидан кенг фойдаланмоқда. Хатто молиявий хизматларни кўрсатишда ҳам интернет дўконларининг таклифи қулайлигини эътироф этадиганлар кўпчиликни ташкил этмоқда. Аммо сир эмас вертуаль оламда чув тушаётганлар ҳам оз эмас.

Шу мақсадга йўналтирилган тарғибот тадбири вилоят Ички ишлар бошқармаси Тезкор қидирув хизмати Киберхавфсизлик бўлими ҳамда алоқадор идоралар ходимлари билан ҳамкорликда ташкил этилди. Масъуллар томонидан таъкидланганидек, Мамлакатимизда 30 мингга яқин интернет фойдаланувчилари борлигини инобатга оладиган бўлсак, уларнинг орасида сиз-у биз ҳам бор, бу кўрсаткич кибер жиноятчилар учун каттагина даромад аудиторияси ҳисобланади.

Мулоқотларда ижтимоий тармоқлар интернет дўконлардан фойдаланишда белгиланган тартиб қоидаларга амал қилмаслик оқибатида фирибгарларнинг тузоғига тушиб қолиш ҳеч гап эмаслиги, пластик карта пинкоди ва паролини шунингдек смс хабарлар орқали юбориладиган махфий кодларни бегона шахсларга бермаслик кераклиги уқтирилши лозим.

Янги Ўзбекистонда барча соҳалари, ижтимоий, иқтисодий, сиёсий соҳалар рақамлаштиришга ўтаётган бир даврда Интернет-маконининг киберхавфсизлигини таъминлашнинг асосий йўналишларини бегилаб берувчи киберхавфсизлик стратегиясини ишлаб чиқилиши лозим. Чунки барча соҳалар

рақамлашиб электрон шаклга ўтар экан электрон ҳукумат ва рақамли иқтисодиёт тизимларига тааллуқли бошқа йўналишлар турли хил киберҳужумлар ва таҳдидларга учраши мумкин. Мазкур соҳаларнинг киберҳужумларга учраши эса мамалакатнинг турли хил соҳаларини издан чиқишига олиб келиши мумкин.

Дарҳақиқат, кибержиноятчилик учун жавобгарлик ҳозирги кундаги Ўзбекистон Республикаси Жиноят кодексида етарлича қамраб олинмаганлиги учун илғор ривожланган хорижий давлатлар жиноят қонунчилиги ва амалиётини ўрганиб ҳозирги кундаги кибержиноятчиликка тегишли барча қилмишларни қамраб оладиган нормаларни амалдаги жиноят қонунчилигимизда мустаҳакамлаш мақсадга мувофиқ бўлади.

Фойдаланилган адабиётлар:

1. Ўзбекистон Республикаси 1999 йил 20 августда қабул қилинган “Телекоммуникациялар тўғрисида”ги 822-1-сонли Қонуни.
2. Н.С.Салаев, Р.Н.Рўзиев. Кибержиноятчиликка қарши курашишга оид миллий ва ҳалқаро стандартлар. Монография. 2018 йил ТДЮУ.

КИБЕРЖИНОЯТЧИЛИККА ҚАРШИ КУРАШНИНГ ҲУҚУҚИЙ АСОСИ СИФАТИДА «КИБЕРХАВФСИЗЛИК ТЎҒРИСИДА»ГИ ҚОНУННИНГ АҲАМИЯТИ

Шоимов Норқобил Бобомуродович

Ўзбекистон Республикаси ИИВ Малака ошириш институти катта ўқитувчиси, юридик фанлар номзоди, доцент

Аннотация. Мақолада ахборот чегара билмас кучга айланиб бораётганлиги, йирик глобал маконга айланган интернет нафақат шахсга, балки жамият ва давлат хавфсизлигига дахл қилувчи қуролга ҳам айланиб улгурганлиги, Ўзбекистон Республикасида киберхавфсизлик борасида кенг кўламли чора-тадбирлар амалга оширилаётганлиги ва бу борада Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида”ги қонунининг аҳамияти ёритиб берилган.

Таянч сўзлар: кибержиноятчилик, кибермакон**,** кибертаҳдид, киберхавфсизлик, киберхавфсизлик объекти, киберхавфсизлик субъекти, киберҳимоя, киберҳужум, муҳим ахборот инфратузилмаси, муҳим ахборот инфратузилмаси объектлари, муҳим ахборот инфратузилмаси субъектлари, қонун**.**

Аннотация: В статье говорится, что информация становится силой, не знающей границ, что Интернет, превратившийся в большое глобальное пространство, стал оружием, затрагивающим не только личную, но и общественную и государственную безопасность, что масштабные меры кибербезопасности становятся реальностью, реализуется в Республике

Узбекистан, и в связи с этим поясняется важность Закона Республики Узбекистан «О кибербезопасности».

Ключевые слова: киберпреступность, киберпространство, киберугроза, кибербезопасность, объект кибербезопасности, субъект кибербезопасности, киберзащита, кибератака, критическая информационная инфраструктура, объекты критической информационной инфраструктуры, субъекты критической информационной инфраструктуры, закон.

Бугунги глобаллашув жараёнида ахборот чегара билмас кучга айланиб, у бутун дунё аҳолисини бошқармоқда. Энг йирик глобал маконга айланган интернет нафақат шахсга, балки жамият ва давлат хавфсизлигига дахл қилувчи қуролга ҳам айланиб улгурди. Хусусан, БМТ Бош Ассамблеяси, Европа Кенгаши, ШҲТ, МДҲ, Араб давлатлари лигаси ва бошқа ташкилотлар томонидан ахборот-коммуникация технологияларидан жиноий мақсадларда фойдаланишга қарши курашиш бўйича минтақавий ва халқаро ҳуқуқий ҳужжатлар қабул қилинган. «We Are Social» ва «Hootsuite» компаниялари «Digital 2021» ҳисоботини тақдим этишди. Унда жаҳонда интернет ва ижтимоий тармоқлар фойдаланувчилари сони қанчага етгани ҳақида маълумот берилган.

2021 йилнинг январь ҳолатига кўра интернетдан 4,66 млрд. киши ёки сайёрамиз аҳолисининг 53,6 фоизи фойдаланмоқда. Ижтимоий тармоқлардан эса 4,2 млрд. киши фойдаланяпти. Ҳисоботда кўрсатилишича, 5,22 млрд. кишининг ёки Ер аҳолисининг 66,6 фоизида шахсий мобил телефонлар бор[1]. Киберхавфсизлик бўйича халқаро экспертлар 2019 йилда киберҳужумлар ҳар 14 секундда содир бўлишини таъкидлади[2]. Ҳар йили кибержиноятчилик оқибатида етказилган моддий зарарнинг миқдори дунё ЯИМнинг 1 % ни ташкил этади[3]. Республикамизда эса, 2023 йилнинг 9 ойида 8734 та мурожаатлар келиб тушган бўлиб, фуқароларга етказилган моддий зарарнинг миқдори уч йилда 372 миллиард 800 млн. сўмни ташкил этган[4].

Юқоридаги мисоллардан маълум бўлмоқдаки, кибержиноятларнинг тарқалиши ва унинг зарари миқдори ошиб, кенг қулоч ёйиб, кундан кунга ривожланиб бормоқда.

Шу сабабли, кибержиноятчиликка қарши курашиш Ўзбекистонда давлат сиёсатининг энг устувор йўналишларидан ҳисобланади. Буни сўнгги йилларда соҳага оид қабул қилинган концептуал аҳамиятга эга норматив-ҳуқуқий ҳужжатлар, кибержиноятчиликнинг олдини олишга қаратилган ислоҳотлар мисолида яққол кўриш мумкин. Жумладан, кибержиноятчиликка қарши курашиш самарадорлигини оширишда Ўзбекистонда амалга оширилаётган ислоҳотларининг асосий ҳужжати ҳисобланган Ўзбекистон Республикаси

[1] https://xabar.uz/texnologiya/dunyoda-internetdan-qancha-odam-fo

[2] S.Morgan. Official Annual Cybercrime Report 2019 // Cybersecurity Ventures.

[3] http://www.statista.com/ (The Statistics Portal).

[4] Бобомуродов Фарход Боймуродович. Кибермаконда содир этилаётган жиноятларга қарши курашишда тезкор-қидирув тадбирларини ўтказилиши – фуқароларнинг ҳуқуқлари ва эркинликларини таъминлашнинг кафолати. // https: //doi.org/10.5281/zenodo.11523262

Президенти ташаббуси билан қабул қилинган 2022 — 2026 йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегиясининг[5] аҳамияти катта ҳисобланади.

Кенг жамоатчилик муҳокамаси натижасида «Ҳаракатлар стратегиясидан — Тараққиёт стратегияси сари» тамойилига асосан ишлаб чиқилган 2022 — 2026 йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегиясининг мамлакатимиз хавфсизлиги ва мудофаа салоҳиятини кучайтириш, очиқ, прагматик ва фаол ташқи сиёсат олиб бориш деб номланган еттинчи устувор йўналишининг 89-мақсадида фуқароларнинг ахборот олиш ва тарқатиш эркинлиги борасидаги ҳуқуқларини янада мустаҳкамлаш ўз аксини топган бўлиб, бунда ахборот соҳасини тартибга солувчи ягона тизимлаштирилган норматив-ҳуқуқий ҳужжат лойиҳасини ишлаб чиқиш, фуқароларнинг ахборот-коммуникация воситаларидан фойдаланиш маданиятини ошириш, шахсий ва сир сақланиши лозим бўлган маълумотларни интернет тармоғида ошкор қилиш билан боғлиқ дахлсизлик ҳуқуқи бузилишининг олдини олиш ҳамда кибержиноятчиликнинг олдини олиш тизимини яратиш муҳим мақсадлардан этиб белгиланган.

Шу мақсадларга эришиш учун 2022 йилнинг 15 апрель куни Ўзбекистон Республикасида киберхавфсизлик соҳасидаги муносабатларни тартибга солишни мақсад қилган Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида”ги ЎРҚ-764-сонли[1] қонун қабул қилинди ва кибержиноятчилик, кибермакон, кибертаҳдид киберхавфсизлик, киберхавфсизлик объекти, киберхавфсизлик субъекти, киберҳимоя, киберҳужум, киберхавфсизликни таъминлашнинг асосий принциплари, киберхавфсизлик соҳасини давлат томонидан тартибга солиш, давлат органлари ва ташкилотларининг киберхавфсизликни таъминлаш борасидаги ҳуқуқ ва мажбуриятлари, маълумотларнинг захира нусхаларини кўчириш, киберхавфсизликни таъминлаш, киберхавфсизлик ҳодисалари, муҳим ахборот инфратузилмаси объектлари, киберхавфсизлик соҳасини қўллаб-қувватлаш ва ривожлантириш ва киберхавфсизлик соҳасидаги халқаро ҳамкорлик масалаларини тартибга солишда мазкур қонуннинг аҳамияти каттадир.

Шуни таъкидлаш лозимки, республикамизда ахборот технологиялари соҳасидаги хавфсизликни таъминлаш, ахборотни эгаллаш, уни ўзгартириш, йўқ қилиш ёки ахборот тизимлари ва ресурсларини ишдан чиқариш, кибермаконда шахс, жамият ва давлат манфаатларини ташқи ва ички таҳдидлардан ҳимоялаш ҳамда киберхавфсизлик ҳодисаларининг олдини олишга, киберҳужумларни аниқлашга ва улардан ҳимоя қилишга, киберҳужумларнинг оқибатларини бартараф этишга, телекоммуникация тармоқлари, ахборот тизимлари ҳамда ресурслари фаолиятининг барқарорлигини ва ишончлилигини тиклашга қаратилган чора-тадбирлар, шунингдек маълумотларни криптографик ва техник

[5] Қонунчилик маълумотлари миллий базаси, 29.01.2022 й., 06/22/60/0082-сон, 18.03.2022 й., 06/22/89/0227-сон, 21.04.2022 й., 06/22/113/0330-сон; 10.02.2023 й., 06/23/21/0085-сон; 03.01.2024 й., 06/24/221/0003-сон.

[1] Қонунчилик маълумотлари миллий базаси, 16.04.2022 й., 03/22/764/0313-сон.

жиҳатдан ҳимоя қилиш чора-тадбирларни кенг халқ оммасига, ижрочиларга тушинтириш, уларнинг бу соҳадаги билимларини мустаҳкамлаб қолмай, балки бу соҳадаги ҳуқуқий саводхонлигини кучайтириш, ҳуқуқий онги ва маънавиятини оширишга ҳам ёрдам беради.

Шу сабабли, ходимлар, ижрочилар, аҳоли, ёшларга ҳуқуқий таълим беришда “Киберхавфсизлик тўғрисида”ги қонуннинг қуйидаги қатор хусусиятларини тушинтириш мақсадга мувофиқдир:

биринчидан, “Киберхавфсизлик тўғрисида”ги қонун киберҳужумларни аниқлашга ва улардан ҳимоя қилишга, киберҳужумларнинг оқибатларини бартараф этишга, шахс, жамият ва давлатнинг манфаатлари ва хавфсизлигини таъминлашда ҳуқуқий манба эканлигини;

иккинчидан, “Киберхавфсизлик тўғрисида”ги қонун бугунги кунда тобора такомиллашиб бораётган “рақамли иқтисодиёт” ва “электрон ҳукумат” тизимини ривожлантириш жараёнида инновацион ресурсларни яратиш билан бир қаторда, ахборот хавфсизлиги, кибермаконда содир этиладиган жиноятларга қарши курашишда ташкилий-техник, операцион ва энг аввало асосий ҳуқуқий манба бўлиши билан бир вақтда, мазкур қонун ўзининг барқарорлиги, нормалари, принциплари ва аҳамияти жиҳатидан узоқ муддатли даврни ҳисобга олиб қабул қилинганлигини;

учинчидан, “Киберхавфсизлик тўғрисида”ги қонун киберхавфсизлик соҳасидаги муносабатларни тартибга солишда янги ҳуқуқий замин ҳисобланиб, суд ҳуқуқ соҳасидаги ислоҳотларни амалга оширишда алоҳида аҳамиятга эга эканлигини.

Шу билан бир қаторда ижрочилар, аҳоли, айниқса ходимларга “Киберхавфсизлик тўғрисида”ги қонуннинг қисқача мазмуни, мақсади ва асосий вазифаларини тушунтириш жоиздир, албатта.

Бинобарин, мазкур қонун 40 моддани ўз ичига олган 8 бобдан иборат бўлиб, унинг 1-боби “Умумий қоидалар” деб номланади. Бу боб 9 та (1-9) моддани ўз ичига олади. Унда ушбу қонуннинг мақсади, киберхавфсизлик тўғрисидаги қонунчилик, ушбу қонунда қўлланиладиган асосий тушунчалар, киберхавфсизликни таъминлашнинг асосий принциплари, яъни қонунийлик, кибермаконда шахс, жамият ва давлат манфаатларини ҳимоя қилишнинг устуворлиги, киберхавфсизлик соҳасини тартибга солишга нисбатан ягона ёндашув, киберхавфсизлик тизимини яратишда маҳаллий ишлаб чиқарувчилар иштирокининг устуворлиги, Ўзбекистон Республикасининг киберхавфсизликни таъминлашда халқаро ҳамкорлик учун очиқ эканлигини етказиш.

Қонуннинг 2 - боби киберхавфсизлик соҳасини давлат томонидан тартибга солишга бағишланган бўлиб, энг авволо ходимларга, ижрочиларга, аҳолига, ёшларга, талаба ва тингловчиларга бу ердаги 10-13-моддаларида берилган киберхавфсизлик соҳасидаги ягона давлат сиёсатини, киберхавфсизлик соҳасидаги ваколатли давлат органи ва бу органнинг ҳуқуқлари ҳамда мажбуриятлари мустаҳкамлаб қўйилганлигини уқдириш лозим.

Қонуннинг 3 - боби “Давлат органлари ва ташкилотларининг киберхавфсизликни таъминлаш борасидаги ҳуқуқ ва мажбуриятлари. Маълумотларнинг захира нусхаларини кўчириш” –деб номланиб, унда давлат

органлари ва ташкилотларининг киберхавфсизликни таъминлаш борасидаги ҳуқуқ ва мажбуриятлари (14-м.), маълумотларнинг захира нусхаларини кўчириш (15-м.) ҳақидаги масалалар ўз аксини топганлигини.

Шунингдек, Қонуннинг 4 - бобида киберхавфсизликни таъминлаш баён этилганлигини ва булар қонуннинг 16-21-моддаларида тўла ўз аксини топганлигини билишлари шарт.

Ходимлар, ижрочилар, аҳоли, ёшлар, талаба ва тингловчиларимиз, қонуннинг "Киберхавфсизлик ҳодисалари" -деб номланган 5 – бобидаги киберхавфсизлик ҳодисаларини текшириш (22-м.), киберхавфсизлик субъектлари томонидан киберхавфсизлик ҳодисалари бўйича чоралар кўриш (23-м.), киберхавфсизлик ҳодисалари тўғрисидаги ахборотни ошкор қилиш (24-м.) масаласи ёритилганлигини билишлари муҳим аҳамиятга эга бўлади.

Ходимлар, ижрочилар, аҳоли, айниқса ёшлар, талаба ва тингловчиларимиз билим олиш жараёнида, "Киберхавфсизлик тўғрисида"ги қонуннинг "Муҳим ахборот инфратузилмаси объектлари" деб номланган 6 – боби 25-31- моддаларида берилган муҳим ахборот инфратузилмаси объектларининг киберхавфсизлигини таъминлашнинг асосий йўналишлари, муҳим ахборот инфратузилмаси объектларини тоифалаштириш, муҳим ахборот инфратузилмаси объектларининг ягона реестри, муҳим ахборот инфратузилмаси субъектларининг ҳуқуқ ва мажбуриятлари, муҳим ахборот инфратузилмаси объектларининг киберхавфсизлигини таъминлаш бўйича талаблар, муҳим ахборот инфратузилмаси объектларининг киберхавфсизлигини таъминлаш тизими ва муҳим ахборот инфратузилмаси объектларининг киберхавфсизлигини баҳолаш масалалари ёритилганлиги билиб олишлари ўта фойдалидир.

Ҳуқуқий билим ва кўникмалар олиш жараёнида мазкур қонуннинг "Киберхавфсизлик соҳасини қўллаб-қувватлаш ва ривожлантириш" деб номланган 7 - боби 32-35-моддаларида қайд этилган киберхавфсизлик субъектларини давлат томонидан қўллаб-қувватлаш, киберхавфсизлик соҳасида илмий-техник ва инновацион фаолиятни қўллаб-қувватлаш, киберхавфсизликни таъминлаш соҳасидаги кадрлар салоҳиятини ривожлантириш ва қўллаб-қувватлаш, муҳим ахборот инфратузилмаси объектларининг киберхавфсизликни таъминлаш учун масъул бўлган ходимларини рағбатлантириш тартиби кўрсатилганлигини билишлари фойдадан холи бўлмайди.

Бундан ташқари, миллий ахборот ресурсларига эга бўлган, улардан фойдаланиш ва уларни тасарруф этиш ҳамда улардан фойдаланиш бўйича электрон ахборот хизматлари кўрсатиш, ахборотни ҳимоя қилиш ҳамда киберхавфсизлик билан боғлиқ муайян ҳуқуқлар ва мажбуриятларга эга бўлган юридик шахс ва якка тартибдаги тадбиркор, шу жумладан муҳим ахборот инфратузилмаси субъектлари қонуннинг "Якунловчи қоидалар" (8-боб, 36-40-м.м.) дея номланган бобидаги киберхавфсизлик соҳасидаги халқаро ҳамкорлик, киберхавфсизлик тўғрисидаги қонунчиликни бузганлик учун жавобгарлик, ушбу Қонуннинг ижросини, етказилишини, моҳияти ва аҳамияти тушунтирилишини таъминлаш, қонунчиликни ушбу қонунга

мувофиқлаштириш ва ушбу қонуннинг кучга кириши каби масалаларнинг ҳуқуқий тартибга солинганлигини ўқиб-ўзлаштириб олишлари жуда муҳимдир. Хулоса қилиб айтганда, миллий ахборот ресурсларига эга бўлган, улардан фойдаланиш ва уларни тасарруф этиш ҳамда улардан фойдаланиш бўйича электрон ахборот хизматлари кўрсатиш, ахборотни ҳимоя қилиш ҳамда киберхавфсизлик билан боғлиқ муайян ҳуқуқлар ва мажбуриятларга эга бўлган юридик шахс ва якка тартибдаги тадбиркор, шу жумладан муҳим ахборот инфратузилмаси субъектларига Ўзбекистон Республикасининг "Киберхавфсизлик тўғрисида"ги қонунини ва унинг мазмун-моҳиятини яхши тушунтириш ва уларнинг ўзлаштириб олишларига эришиш лозим. Шундагина ҳар бир интернет фойдаланувчиси ва хизмат кўрсатувчилар кибер оламда ҳам ҳаётдаги каби эҳтиёткорликни унутмасалар, аксарият кибержиноятларнинг олди олинган бўлар эди.

QO‘RIQLANADIGAN OBYEKTLARDA O‘RNATILGAN VIDEO TASVIRLARDAGI SHOVQINLAR DARAJASINI BAHOLASH:USUL VA ALGORITMLAR

Abdulloyev Daler Amrilloyevich

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti magistratura tinglovchisi

Bugungi kunda qo‘riqlanuvchi obyektlar xavfsizligini ta’minlashda muhim ahamiyatga ega hududlarni texnik kuzatish vositalarining o‘rni tobora kengayib, hal qiluvchi rol o‘ynamoqda. Shu boisdan texnik kuzatuv vositalarining imkoniyatlarini oshirishga alohida e‘tibor qaratilmoqda.

Videokuzatuv vositalari bugunga kelib faqat kuzatish, yozib olish va saqlash bilangina cheklanib qolmadi, balki kuzatuv hududidagi yuqori massivli o‘zgarishlar asosida xabarlarni, tashvish signallarini ham shakllantirish kabi vazifalarni bajarmoqda.

Ma’lum bo‘lishicha, videokuzatuv vositalari kuzatish, yozib olishdan tashqari, videomateriallar yordamida kuzatuv hududidagi tartibbuzarlik haqidagi ma’lumotlar tahlilini olib borishga hissa qo‘shadi. Ular nafaqat pult operatori balki bir vaqtning o‘zida tegishli buyruq talablariga muvofiq obyekt ma’muriyati, qorovul boshlig‘i, shtab, qo‘mondonlik punktlariga va boshqa ruxsat etilgan joylarga videomateriallarni uzatish imkoniyatiga va shu tariqa voqea joyidan o‘ziga xos ishonchli ma’lumotlar manbayi hisoblanmoqda.

Biroq, turli xil shovqin manbalari tufayli yuqori sifatli videoni suratga olishda qiyinchiliklar tug‘ilmoqda. Video tasvirlardagi shovqin past yoki yuqori yorug‘lik sharoitlari, kamera sensori cheklovlari, siqish algoritmlari va uzatishdagi xatoliklar kabi omillardan kelib chiqishi mumkin. Video tasvirlardagi shovqin darajasini baholash olingan kadrlarning sifatini yaxshilash va boshqarish hamda shovqinni kamaytirish uchun tegishli choralarni ko‘rish uchun juda muhimdir. Ushbu maqolada video tasvirlardagi shovqinni baholash uchun ishlatiladigan usullar, ularning ahamiyati va videoni qayta ishlashga ta’siri o‘rganilgan.

Video tasvirlardagi shovqinlar xususiyatlariga koʻra kadr piksellariga turlicha ta’sir koʻrsatadi:

Gauss shovqini: Gauss shovqini — bu tasodifiy signalga qoʻshilgan, oʻrtacha qiymati 0 va dispersiyasi (variansi) belgilangan, normal taqsimotga ega boʻlgan shovqindir. Bunday shovqin signalga teskari ta’sir koʻrsatib, uni buzishi mumkin. Gauss shovqini tasodifiy oʻzgaruvchilar normal taqsimotga ega boʻlib, uning taqsimotining oʻrtacha qiymati (mu) va dispersiyasi (sigma²) belgilangan. Gauss taqsimoti simmetrik boʻlib, uning grafigi halqaga oʻxshaydi. Gauss shovqini koʻplab tabiiy va texnik jarayonlarda uchraydi, masalan, tasodifiy xatoliklar, ma’lumot uzatishdagi buzilishlar va boshqalar.

Misol uchun, tasavvur qiling, biror sensor ma’lum bir oʻzgarishni oʻlchashda oʻzi xatolik qilishi mumkin. Agar bu xatoliklar tasodifiy va normal taqsimlangan boʻlsa, u holda shovqin “Gauss shovqini” sifatida tavsiflanadi. Matematikaning va signallarni qayta ishlashning turli sohalarida Gauss shovqini model sifatida juda muhimdir.

Siqish algoritmlari: videoni siqish paytida kiritilgan algoritmlarning toʻliq qamrab olmasligi sababli buzilishlar, blokirovka yoki xiralashishga olib keladi.

Shovqinni baholashning ahamiyati quyidagilarni amalga oshirishda yuqori hisoblanadi:

sifatni baholashda shovqin darajasini baholash shovqinning video sifatiga ta’sirini aniqlashga yordam beradi, tasvir sifatini baholash va taqqoslashda yordam beradi.

Shovqinni kamaytirish: shovqinni aniq baholash video ravshanligini yaxshilash va artefaktlarni kamaytirish uchun tegishli denoising usullarini tanlashga rahbarlik qiladi.

Qayta tiklash va takomillashtirish: shovqin xususiyatlarini baholash video tasvirlarni tiklash va yaxshilash uchun samarali algoritmlarni ishlab chiqishda yordam beradi.

Tarkibni tahlil qilish: shovqinni baholash video kontentning degradatsiyasi haqida tushuncha berishi, obyektni aniqlash va kuzatish kabi vazifalarni osonlashtirishi mumkin.

Shovqinni baholash usullari:

Statistik koʻrsatkichlar: oʻrtacha, standart ogʻish va gistogrammaga asoslangan yondashuvlar kabi piksel intensivligini statistik tahlil qilish shovqin xususiyatlarini miqdoriy baholashni ta’minlaydi.

Chastotani domenini tahlil qilish: video tasvirning chastota komponentlarini tahlil qilish uchun Fourier yoki toʻlqinli transformatsiyalardan foydalanish, shovqinni baholash va olib tashlashga imkon beradi. Chastotani domen tahlilidagi eng muhim kontseptsiya - bu transformatsiya.[62]

Vaqtinchalik tahlil: shovqin naqshlarini aniqlash va shovqin darajasini baholash uchun ketma-ket ramkalar orasidagi vaqtinchalik muvofiqlikni tahlil qilish.

Mashinani oʻrganish yondashuvlari: shovqin naqshlarini oʻrganish va koʻrinmaydigan video ramkalardagi shovqin darajasini bashorat qilish uchun etiketli shovqinli va toza video ma’lumotlardan foydalangan holda oʻqitish modellari.

[62] https://uz.maywoodcuesd.org/difference-between-time-domain-and-vs-frequency-domain-3745

Eksperimental baholash va qiyosiy tadqiqotlar:

Turli xil shovqin darajalari va turlari bilan benchmark video ma’lumotlar to‘plamlarida tajribalar o‘tkazish.

Shovqinni baholashning turli usullarini aniqlik, mustahkamlik va hisoblash samaradorligi bo‘yicha taqqoslash.

Shovqinni baholash algoritmlarining ishlashini ularning bashoratlarini yer haqiqati shovqin darajalari bilan taqqoslash orqali baholash.

Videoni qayta ishlashda shovqinni baholashning qo‘llanilishi:

Video Denoising: denoising algoritmlarini tanlash va optimallashtirishga rahbarlik qilish, vizual sifatni yaxshilash uchun shovqinni baholash natijalaridan foydalanish.

Videoni takomillashtirish: tafsilotlarni saqlash va artefaktlarni kamaytirish uchun shovqin xususiyatlariga asoslangan takomillashtirish texnikasini moslashtirish.

Videoni siqish: shovqinni yaxshiroq saqlash va artefaktni kamaytirish uchun siqishni algoritmlarini optimallashtirish uchun shovqinni baholashni o‘z ichiga oladi.

Xulosa:

Bugungi kunda videokuzatuv tizimlari nafaqat kuzatish va yozib olish funksiyalarini bajaribgina qolmay, balki yuqori darajadagi tahlil, xabar yuborish va signal shakllantirish vazifalarini ham amalga oshirmoqda. Shu bilan birga, videokuzatuv tizimlarida yuzaga keladigan shovqinlar, masalan, Gauss shovqini, siqish algoritmlari yoki kam yorug‘lik sharoitlari kabi muammolar videolarning sifatiga salbiy ta’sir ko‘rsatmoqda. Shovqinlarni baholash va kamaytirish, video tasvirlarning sifatini yaxshilash, artefaktlarni kamaytirish va videoni qayta ishlashning samaradorligini oshirishda katta ahamiyatga ega.

Shovqin darajasini aniqlash va baholashda foydalaniladigan usullar, masalan, statistik tahlil, chastota domenini tahlil qilish, vaqtinchalik tahlil va mashinani o‘rganish yondashuvlari, videokuzatuv tizimlarining sifatini oshirish uchun asosiy vositalar sifatida xizmat qiladi. Ushbu usullar videoni takomillashtirish, denoising (shovqinni kamaytirish) va siqish algoritmlarini optimallashtirishda muhim rol o‘ynaydi.

Shovqinni baholashning turli usullarini taqqoslash, ularning samaradorligini sinovdan o‘tkazish va turli shovqin turlari bilan ishlash orqali video tasvirlarining sifatini yaxshilash mumkin. Bu, o‘z navbatida, obyektlarni kuzatish, tartibbuzarliklarni aniqlash va boshqa xavfsizlik vazifalarini samarali bajarish imkonini beradi.

Umuman olganda, video tasvirlardagi shovqinlarni baholash va boshqarish texnologiyalari, xavfsizlikni ta’minlash, ma’lumotlarni uzatish va video kontentni qayta ishlashda yirik ahamiyatga ega bo‘lib, zamonaviy videokuzatuv tizimlarining samaradorligini oshirishda muhim omil bo‘ladi.

Foydalanilgan adabiyotlar:

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений. – М.: Техносфера, 2005. – 1072 с.

2. Tashmanov E.B., Xursandov E.D. Methods for filtering image pulse noise in video information systems // Journal of Hunan University（Natural Sciences）Vol. 49. No. 10 October 2022. p.1685-1689.

3. Иванов А., Смирнова Е. Цифровая обработка кадров видеоизображений: современные подходы и тенденции.
4. https://uz.maywoodcuesd.org/difference-between-time-domain-and-vs-frequency-domain-3745

АХБОРОТ ТЕХНОЛОГИЯЛАРИ СОҲАСИДАГИ ҲУҚУҚБУЗАРЛИКЛАР ВА ЖАВОБГАРЛИК МАСАЛАЛАРИ

Ганиев Шахобиддин Холматович

Ўзбекистон Республикаси ИИВ Малака ошириш институти Юридик фанлар кафедраси катта ўқитувчиси
тел: +99890-317-10-27, shax.ganiev86@gmail/com

Аннотация. Ушбу мақолада ахборот технологиялари соҳасидаги ҳуқуқбузарликлар тушунчаси, турлари, жавобгарлик масалалари, унга қарши курашиш бўйича амалга оширилиши керак бўлган чора-тадбирлар, шунингдек унинг самарали жиҳатларига эътибор қаратилган.

Таянч сўзлар: кибержиноят, киберхавфсизлик, кибермакон, ахборот хавфсизлиги, ахборот технологиялари, ҳуқуқбузарлик, жиноят, статистика.

Бугунги кунда замон шиддат билан ривожланиб бораётгани сари инсонларнинг ҳамда жамият ҳаёти тубдан ўзгариб бораётганини ва барча соҳаларда ахборот технологиялари ва Интернетдан кенг фойдаланиш кундалик фаолиятнинг бир қисми бўлиб қолганлигини кўришимиз мумкин. Шунингдек, интернет замонавий инсоннинг фикрлаш тарзига ва амалий фаолиятига ўзининг ижобий таъсири билан кириб келди. Ахборот технологиялари ва интернет тармоқлари ривожланиб борар экан, албатта унинг ижобий ва самаралари жиҳатларидан ташқари, қонунга хилоф равишда (рухсатсиз) ахборот тизимига кириб ёки ундан фойдаланган ҳолда содир этилаётган ҳуқуқбузарликларнинг салмоғини ошиши тенденцияси кузатилмоқда. Айниқса, ахборот технологияларидан фойдаланган ҳолда ижтимоий тармоқларда сайтларни бузиб кириш, вирусли дастурлар тарқатиш каби ҳолатлар кўп учраётгани бутун дунёни ташвишга солиб келмоқда. Бу ҳолат эса, жамият ҳаётининг бир нечта соҳаларига бир вақтнинг ўзида кириб борадиган жиддий таҳдид мавжудлиги ҳақида хулоса қилиш имконини беради, чунки у фуқароларнинг ҳуқуқ ва эркинликларига ҳам, бутун мамлакат иқтисодиётига ҳам катта таъсир қилади.

Шу боис, 2021 йил 17 сентябрь куни Тожикистон пойтахти Душанбе шаҳрида ўтказилган Шанхай ҳамкорлик ташкилоти Давлат раҳбарлари кенгашининг юбилей мажлисида Президентимиз Ш.М.Мирзиёев “кибермакондаги замонавий таҳдид ва хатарларга муносиб жавоб қайтариш учун ШҲТнинг ахборот хавфсизлиги соҳасидаги экспертлар форумини таъсис этиш тўғрисида[63]” ташаббус билан чиққан эди.

[63] https://daryo.uz/k/2021/09/17/shavkat-mirziyoyev-shht-majlisida-kibermakondagi-tahdidlarga-qarshi-axborot-xavfsizligi-sohasidagi-ekspertlar-forumini-tasis-etishni-ilgari-surdi.

Ушбу мақолани ёритишдан даставвал “кибержиноятчилик”, “киберхавфсизлик”, “кибермакон” каби сўзларнинг терминологок тушунчаларига тўхталиб ўтишимиз ва уларнинг мазмунини тушуниб олишимиз мақсадга мувофиқдир, негаки ижтимоий ва бошқа юридик адабиётларда мазкур терминлар турлича талқин қилинади.

Жумладан, ***кибержиноятчилик*** деганда, ахборотни эгаллаш, уни ўзгартириш, йўқ қилиш ёки ахборот тизимлари ва ресурсларини ишдан чиқариш мақсадида кибермаконда дастурий таъминот ва техник воситалардан фойдаланилган ҳолда амалга ошириладиган жиноятлар йиғиндиси тушунилади.

Киберхавфсизлик деганда эса, кибермаконда шахс, жамият ва давлат манфаатларининг ташқи ва ички таҳдидлардан ҳимояланганлик ҳолатини тушуниш лозим. Шунингдек, ***кибермакон*** - ахборот технологиялари ёрдамида яратилган виртуал муҳитни тушуниш мумкин[64].

Энг ташвишли томони шундан ибортаки, ахборот технологиялари соҳасидаги ҳуқуқбузарликларнинг шакллари кўп қиррали бўлиб, технологиялар ва Интернетнинг доимий ривожланиши билан унинг содир этиш усуллари ҳам тобора ортиб бормоқда.

Шу сабабли, “2022-2026 йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегияси”нинг **89-мақсади**: “Фуқароларнинг ахборот олиш ва тарқатиш эркинлиги борасидаги ҳуқуқларини янада мустаҳкамлаш. Ахборот соҳасини тартибга солувчи ягона тизимлаштирилган норматив-ҳуқуқий ҳужжат лойиҳасини ишлаб чиқиш. Фуқароларнинг ахборот-коммуникация воситаларидан фойдаланиш маданиятини ошириш. Шахсий ва сир сақланиши лозим бўлган маълумотларни Интернет тармоғида ошкор қилиш билан боғлиқ дахлсизлик ҳуқуқи бузилишининг олдини олиш. Кибержиноятчиликнинг олдини олиш тизимини яратиш”[65] деб белгилаб қўйилган.

Ўзбекистон Республикаси миқёсида содир этилган жиноятлар статистикасининг таҳлилига кўра, 2023 йилнинг 11 ойида жами 5,5 (беш ярим) мингта кибержиноят содир этилган бўлиб, шулардан 70 фоизи банк карталари билан боғлиқ ҳолда содир этилган фирибгарлик ва ўғирлик жиноятлари эканлиги маълум бўлган. Мазкур жиноятларнинг сабаблари ва уларнинг содир этилишига имкон берган шарт-шароитларнинг таҳлилига кўра мамлакатимиздаги 50 га яқин тўлов тизими бўлиб, уларнинг ҳаммаси ҳам киберхавфсизлик талабларига жавоб бермаслиги қайд этилган[66].

Шу сабабли ҳам далатимиз раҳбари Ш.М.Мирзиёев барча электрон тўлов тизимлари учун ягона киберхавфсизлик талабларини ишлаб чиқиш топшириғини берган эди.

---

[64] Ўзбекистон Республикасининг 2022 йил 15 апрелдаги “Киберхавфсизлик тўғрисида”ги ЎРҚ-764-сон Қонуни. (Қонунчилик маълумотлари миллий базаси, 16.04.2022 йил, 03/22/764/0313-сон).

[65] Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги “2022-2026 йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида”ги ПФ-60-сон Фармони (Қонунчилик маълумотлари миллий базаси, 03.01.2024 й., 06/24/221/0003-сон).

[66] https://www.gazeta.uz/uz/2023/12/21/cyber-crime/

Ўзбекистон Республикаси миллий қонунчилигида ахборот технологиялари соҳасида содир этилаётган ҳуқуқбузарликлар учун маъмурий ва жиноий жавобгарликлар белгиланган бўлиб, унга кўра Ўзбекистон Республикаси Маъмурий жавобгарлик тўғрисидаги кодекснинг “Транспортдаги, йўл хўжалиги ва алоқа соҳаларидаги ҳуқуқбузарликлар учун маъмурий жавобгарлик” деб номланган XI-бобининг 155-155^5-моддаларида ахборот технологиялари соҳасига оид 6 та турдаги маъмурий ҳуқуқбузарликлар ўз аксини топган. Жумладан:

155-модда. Ахборотдан фойдаланиш қоидаларини бузиш

Ахборот тизимидан фойдаланиш мақсадида унга рухсатсиз кириб олишда ифодаланган ахборот ва ахборот тизимларидан фойдаланиш қоидаларини бузиш —

155^1-модда. Компьютер тизимидан фойдаланиш қоидаларини бузиш

Компьютер тизимидан фойдаланишга рухсати бўлган шахснинг ушбу тизимдан фойдаланишнинг белгиланган қоидаларини бузиши компьютер ахборотининг йўқ қилиб юборилишига, тўсиб қўйилишига, модификациялаштирилишига, компьютер ускунаси ишлашининг бузилишига сабаб бўлса, —

155^2-модда. Телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш

Телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш, жиноят аломатлари мавжуд бўлмаган тақдирда —

155^3-модда. Мобиль қурилманинг халқаро ўзига хос идентификация кодини ёки абонент қурилмасининг идентификациялаш модулини қонунга хилоф равишда ўзгартириш

Мобиль қурилманинг халқаро ўзига хос идентификация кодини қонуний ишлаб чиқарувчининг рухсатисиз ўзгартириш, худди шунингдек ушбу мақсадда махсус дастурларни ишлаб чиқиш, тарқатиш ёки улардан фойдаланиш, —

155^4-модда. Крипто-активлар айланмаси соҳасидаги қонунчиликни бузиш

Крипто-активларни қонунга хилоф равишда олиш, ўтказиш ёки айирбошлаш, белгиланган тартибда лицензия олмасдан крипто-активлар айланмаси соҳасидаги хизматлар провайдерлари фаолиятини амалга ошириш, —

155^5-модда. Майнинг фаолиятини қонунга хилоф равишда амалга ошириш

Майнинг фаолиятини белгиланган тартибни бузган ҳолда амалга ошириш[67].

Ўзбекистон Республикаси Жиноят кодексининг “Ахборот технологиялари соҳасидаги жиноятлар” деб номланган XX^1-бобининг 278^1-278^9-моддаларида 9 та турдаги жиноятлар белгилаб қўйилган. Хусусан:

278^1-модда. Ахборотлаштириш қоидаларини бузиш

Ахборотлаштириш қоидаларини бузиш, яъни белгиланган ҳимоя чораларини кўрмаган ҳолда ахборот тизимлари, маълумотлар базалари ва банкларини, ахборотга ишлов бериш ҳамда уни узатиш тизимларини яратиш, жорий этиш ва улардан фойдаланиш ҳамда ахборот тизимларидан рухсат билан фойдаланиш

[67] Ўзбекистон Республикасининг Маъмурий жавобгарлик тўғрисидаги кодекс (Қонунчилик маълумотлари миллий базаси, 22.11.2024 й., 03/24/1004/0948-сон).

фуқароларнинг ҳуқуқларига ёки қонун билан қўриқланадиган манфаатларига ёхуд давлат ёки жамоат манфаатларига кўп миқдорда зарар ёхуд жиддий зиён етказилишига сабаб бўлса, —

278[2]-модда. Компьютер ахборотидан қонунга хилоф равишда (рухсатсиз) фойдаланиш

Компьютер ахборотидан, яъни ахборот-ҳисоблаш тизимлари, тармоқлари ва уларнинг таркибий қисмларидаги ахборотлардан қонунга хилоф равишда (рухсатсиз) фойдаланиш, агар ушбу ҳаракат ахборотнинг йўқ қилиб юборилиши, тўсиб қўйилиши, модификациялаштирилиши, ундан нусха кўчирилиши ёхуд унинг қўлга киритилишига, электрон ҳисоблаш машиналари, электрон ҳисоблаш машиналари тизими ёки уларнинг тармоқлари ишининг бузилишига сабаб бўлса, —

278[3]-модда. Компьютер тизимидан, шунингдек телекоммуникация тармоқларидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш

Ҳимояланган компьютер тизимидан, шунингдек телекоммуникация тармоқларидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус дастурий ёки аппарат воситаларини ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш —

278[4]-модда. Компьютер ахборотини модификациялаштириш

Компьютер ахборотини модификациялаштириш, яъни компьютер тизимида сақланаётган ахборотни қонунга хилоф равишда ўзгартириш, унга шикаст етказиш, уни ўчириш, худди шунингдек била туриб унга ёлғон ахборотни киритиш фуқароларнинг ҳуқуқларига ёки қонун билан қўриқланадиган манфаатларига ёхуд давлат ёки жамоат манфаатларига кўп миқдорда зарар ёхуд жиддий зиён етказилишига сабаб бўлса, —

278[5]-модда. Компьютер саботажи

Ўзганинг компьютер ускунасини ёки хизматда фойдаланиладиган компьютер ускунасини қасддан ишдан чиқариш, худди шунингдек компьютер тизимини бузиш (компьютер саботажи) —

278[6]-модда. Зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш

Компьютер тизимида сақланаётган ёки узатилаётган ахборотни рухсатсиз йўқ қилиб юбориш, тўсиб қўйиш, модификациялаштириш, ундан нусха кўчириш ёки уни қўлга киритиш мақсадини кўзлаб компьютер дастурларини яратиш ёки мавжуд дастурларга ўзгартиришлар киритиш, худди шунингдек махсус вирус дастурларини ишлаб чиқиш, улардан қасддан фойдаланиш ёки уларни қасддан тарқатиш —

278[7]-модда. Телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш

Ўрнатилган ҳимоя тизимларини четлаб ўтган ҳолда телекоммуникация тармоғидан фойдаланиш ва халқаро трафикни ўтказиш мақсадида телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш, шунингдек мазкур мақсадлар учун мўлжалланган махсус дастурий ёки аппарат

воситаларини қонунга хилоф равишда (рухсатсиз) сақлаш ва уларнинг фаолият кўрсатиши учун шароитлар яратиш —

278[8]-модда. Крипто-активлар айланмаси соҳасидаги қонунчиликни бузиш

Крипто-активларни қонунга хилоф равишда олиш, ўтказиш ёки айирбошлаш, белгиланган тартибда лицензия олмасдан крипто-активлар айланмаси соҳасидаги хизматлар провайдерлари фаолиятини амалга ошириш ёхуд крипто-активлар айланмаси соҳасидаги хизматлар провайдерлари томонидан аноним крипто-активлар билан операцияларни амалга ошириш шундай ҳаракатлар учун маъмурий жазо қўлланилганидан кейин содир этилган бўлса, —

278[9]-модда. Майнинг фаолиятини қонунга хилоф равишда амалга ошириш

Аноним крипто-активлар майнинги билан шуғулланиш ёки белгиланган тартибни бузган ҳолда майнинг фаолиятини амалга ошириш шундай ҳаракатлар учун маъмурий жазо қўлланилганидан кейин содир этилган бўлса, —

Бундан ташқари, Жиноят кодекси Махсус қисмининг тегишли моддаларида кўрсатиб ўтилган жиноятлар қонунга хилоф равишда (рухсатсиз) ахборот тизимига кириб ёки ундан фойдаланган ҳолда содир этилса, ўша модда бўйича оғирлаштирувчи ҳолат сифатида жиноий жавобгарлик белгилаб қўйилган.

Хулоса сифатида қайд этиш лозимки, ҳуқуқни мухофаза қилувчи органлар томонидан амалга ошириб келинаётган ҳуқуқий тарғиботлар давомида кибержиноятчиликка қарши курашиш бўйича аҳолининг ҳуқуқий онги ва ҳуқуқий маданиятини юксалтириш, кибержиноятга нисбатан муросасиз муносабатни шакллантириш лозим. Шунингдек, давлат ва жамият ҳаётининг барча соҳаларида кибержиноятнинг олдини олишга доир чора-тадбирларни амалга ошириш, кибержиноятга оид ҳуқуқбузарликларни ўз вақтида аниқлаш, уларга чек қўйиш, уларнинг оқибатларини, уларга имкон берувчи сабаблар ва шарт-шароитларни бартараф этиш, кибержиноятга оид ҳуқуқбузарликларни содир этганлик учун жавобгарликнинг муқаррарлиги принципини таъминлаш чоралари ўз вақтида сифатли амалга оширилса, бу турдаги жиноятларни содир этилишини олди олинишига замин яратилади.

Фойдаланилган адабиётлар:

1. Ўзбекистон Республикаси Конституцияси – Т.: 2024.
2. Ўзбекистон Республикаси Маъмурий жавобгарлик тўғрисида кодекс – Т.: 2024.
3. Ўзбекистон Республикаси Жиноят кодекси – Т.: 2024.
4. Ўзбекистон Республикасининг 2022 йил 15 апрелдаги “Киберхавфсизлик тўғрисида”ги ЎРҚ-764-сон Қонуни.
5. Ўзбекистон Республикаси Президентининг 2022 йил 22 январь кунидаги “2022-2026 йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида”ги ПФ-60-сон Фармони.
https://daryo.uz/k/2021/09/17/shavkat-mirziyoyev-shht-majlisida- kibermakondagi-tahdidlarga-qarshi-axborot-xavfsizligi-sohasidagi-ekspertlar-forumini-tasis-etishni-ilgari-surdi

АХБОРОТ ТЕХНОЛОГИЯЛАРИ СОҲАСИДАГИ ЖИНОЯТЛАРНИ ОЛДИНИ ОЛИШ ВА УЛАРГА ҚАРШИ КУРАШИШ ДАВР ТАЛАБИ

Аҳмедов Ислом Бахтиёр ўғли

Ўзбекистон Республикаси ИИВ МОИ Махсус фанлар кафедраси бошлиғи ўринбосари, доцент

Аннотация. Мақолада ахборот технологиялари соҳасидаги жиноятлар, уларнинг турлари, энг кўп содир этиладиган кўринишлари ҳамда уларни олдини олиш ва қарши курашиш масалалари ёритилган.

Калит сўзлар: ахборот технологиялари, ахборот технологиялари соҳасидаги жиноятлар, кибержиноятлар, фишинг, фарминг, кетфишинг жиноятларни олдини олиш ва уларга қарши курашиш.

ПРЕДУПРЕЖДЕНИЕ И БОРЬБА С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ – ТРЕБОВАНИЕ ВРЕМЕНИ

Аннотация. В статье рассматриваются преступления в сфере информационных технологий, их виды, наиболее распространенные формы, а также вопросы предупреждения и борьбы с ними.

Ключевые слова: информационные технологии, преступления в сфере информационных технологий, киберпреступления, фишинг, фарминг, кетфишинг, профилактика и борьба с преступностью.

PREVENTION AND COMBATING CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY IS A NEED OF THE TIME

Annotation. The article discusses crimes in the field of information technology, their types, the most common forms, and issues of preventing and combating them.

Keywords: information technology, information technology crimes, cybercrimes, phishing, pharming, ketphishing, crime prevention and combating.

Шиддат билан ривожланаётган асримизнинг глобал муаммолари тоифасига янгидан-янги турлари пайдо бўлаётган ахборот технологиялари соҳасидаги жиноятлар яъни, қисқача қилиб айтганда кибержиноятчилик ҳисобланади. Бундай жиноятларнинг кенг тарқалган қуйидаги кўринишларини эътироф этишимиз мумкин, вирусли дастурларни тарқатиш, паролларни бузиб кириш, кредит карта ва бошқа банк реквизитларидаги маблағларни ўзлаштириш, талон-торож қилиш, шунингдек, интернет орқали қонунга зид ахборотлар, хусусан, туҳмат(бўҳтон), ҳақоратли, маънавий бузуқ, порнографик, зўровонликни тарғиб қилувчи маълумотларни тарқатиш билан инсоният айниқса, ёшларни соғлиғига, мол-мулкига энг хавфлилиги ҳаётига катта хавф солаётгани кўз юма олмаймиз.

«Кибержиноятчилик» тушунчаси ахборот-коммуникация технологиялари воситаларидан фойдаланган ҳолда, виртуал тармоқда даҳшат солиш, вирус ва

бошқа зарарли дастурлар, қонунга зид ахборотлар тайёрлаш ва тарқатиш, электрон хатларни оммавий тарқатиш (спам), хакерлик ҳужуми, веб-сайтларга ноқонуний кириш, фирибгарлик, маълумотлар бутунлиги ва муаллифлик ҳуқуқини бузиш, кредит карточкалари рақами ҳамда банк реквизитларини ўғирлаш (фишинг ва фарминг) ва бошқа турли қонунбузарликлар билан изоҳланади. Мазкур қилмишларнинг айримларини кўриб чиқадиган бўлсак.

Фишинг (phishing) – бу кибержиноятчилар томонидан фойдаланувчиларнинг конфиденциал маълумотлари (кредит карта маълумотларини, фойдаланувчи номларини, пароллар ва бошқа)ни тўплаш учун фойдаланиладиган интернет фирибгарлигининг кўриниши. Интернет-фирибгарлари жабрланувчиларни ишонишга ва махфий маълумотларини ошкор қилишга мажбурлаш учун ўзларини ишончли юридик шахс ёки давлат идоралари ходими сифатида кўрсатадилар.

Асосан соҳта аккаунтлар орқали ижтимоий тармоқлардан турли хил хизматларни таклиф қилиб, пул ўтказишларини сўрашмоқда. Афсуски, бундай таклифларга ишониб қолганлар топилмоқда. Фирибгарлар уларни пулларини ўзлаштириб, ғойиб бўлишмоқда.

Мисол учун: бир кишининг электрон почтасига Африканинг Того давлатидан Абрахам Смит деган кимсадан хат келибди. Ўзини адвокат деб таништирган бу номаълум шахс рус тилида саводсизларча битилган мактубида 93 ёшли бадавлат Вероника Палмер исмли аёл номидан иш юритиб, унинг топшириғига биноан муносиб меросхўр топиш кераклигини маълум қилган. **“Илмоқли”** таклиф, жаноб А.Смит ўз хатида “меросхўр”ни топиш борасидаги кўп йиллик изланишлардан сўнг “Facebook” ижтимоий тармоғида шу кишининг анкетаси ва қизиқишлари билан танишгач, турли номзодлар орасидан айнан уни танлаганини билдирган. Хатда адвокат ушбу шахс ўзи ҳақидаги барча зарур маълумотларни, жумладан, мобил ва уй телефони рақами, паспорт маълумотлари, банкдаги ҳисоб-рақамини иложи борича тезроқ юборишни илтимос қилган. Буларнинг барчаси гўё васиятномани “расмийлаштириш” учун керак бўлар эмиш.

Гап нима ҳақида бораётганини яхши англаган шахс, бу қизиқ воқеанинг оқибатини билиш мақсадида ёлғон ахборот жўнатди. Жавоб ҳам ўзини кўп куттирмади. Бир неча кун ўтгач, адвокат “меросхўр”ни васиятномани расмийлаштиришга оид барча жараёнлар “муваффақиятли бажарилгани” билан табриклаб, “Web Money” электрон тўлов тизими орқали ўз хизматлари учун 2 минг АҚШ доллари тўлаб қўйишини сўрайди. “Палмер хоним ҳозирги пайтда ўз маблағини тасарруф этадиган ҳолатда эмас ва унинг вафотидан сўнг бу маблағ сизга мерос бўлиб ўтади. Кўрсатилган маблағни тўлаганингиздан кейин бу ерга келиб, хоним билан танишишингиз мумкин”, деб ёзилган ўша сирли мактубда.

Фарминг (pharming) – соҳта сайтлар орқали фойдаланувчилар маълумотларини ўғирлашдир.

Кетфишинг (catfishing) – интернетда ёки бутун ижтимоий тармоқлардаги гурухларда эмоционал (романтик) муносабатларда одамларни алдаш мақсадида, сохта профиль, аккаунт ёки веб-сайтлардан фойдаланган ҳолда мулоқотга киришиб, ўз мақсадларига эришишни ўз ичига олган жараён.

Мутахассислар “Кетфишинг”да шахсдаги қуйидаги ҳолатлар асосида кўпинча содир этилишини эътироф этишади: ўта қизиқувчанлик, зерикиш(бекорчилик), ёлғизлик, нафрат, қасос(ўч олиш).

“Кетфишинг”дан кўзланган мақсад, худди фишингда учрагани каби, ҳар 10 та ҳолатдан 9 тасида жабрланувчиларнинг пул маблағларини эгаллаш ёки шахсий маълумотларни ўзлаштириб, уларни тарқатиш билан товламачилик қилиш ҳаракатларини ўз ичига олади.

Умуман олганда, кибертерроризм ва унинг жамият ҳаётига солаётган хавфининг кўлами ҳам ошиб бораётганини таъкидлаш жоиз.

Кибертеррористик ҳаракат (киберҳужумлар) – компьютерлар ва ахборот коммуникация воситалари ёрдамида амалга оширилган, одамларнинг ҳаёти ва соғлиғига бевосита хавф туғдирадиган ёки потенциал хавф туғдириши мумкин бўлган, моддий обьектларга катта зарар етказиши ёки шунга олиб келиши мумкин бўлган, ижтимоий хавфли оқибатларнинг бошланиши ёки мақсади бўлган сиёсий сабаблардир.

Замонавий террорчилар учун кибермакондан фойдаланишнинг қулайлиги киберҳужумни амалга ошириш катта молиявий харажатларни талаб қилмаслиги, яширинлиги билан боғлиқ. Экспертларнинг хулосасига кўра, бу ривожланаётган давлатларнинг тараққиётига кўмаклашиш, умуминсоний демократик тамойилларни қарор топтириш ниқоби остида фуқаролар онгига таьсир ўтказиш, уларни турли йўллар билан ўз мақсадлари сари бўйсундириш орқали амалга оширилмоқда.

Афсуски, бу жараёнда киберҳужумларни уюштириш, бу йўлда интернет глобал тармоғининг мислсиз имкониятларидан «самарали» фойдаланишга уринишлар тобора авж олмоқда.

Интернетда мавжуд ижтимоий тармоқлар, уларнинг ишлаб чиқарувчилари ва ҳомийларининг суверен давлат ички ишларига «аралашишлари» қандай рол ўйнаши охиригача ўрганилмаганлиги боис баьзан бундай «аралашув» мазкур давлатга қарши эканлиги ҳали ҳануз эьтироф этилгани йўқ.

Ижтимоий тармоқлар эгалари ушбу тармоқлар саҳифаларида давлат тузумини ағдаришга даьват қилингани учун жавобгарликка тортилишининг халқаро миқёсдаги ҳуқуқий асослари яратилмаган. Ваҳоланки, ҳар бир қилинган жиноий ҳатти-ҳаракат ёки ҳаракатсизлик мазмун-моҳиятига кўра, албатта, жавобсиз ва жазосиз қолмаслиги керак. Интернет сайтлари тўсатдан пайдо бўлиб, кўпинча форматини, сўнгра манзилини ўзгартиради. Шу боис айрим мутахассислар интернетнинг буткул очиқлиги каби дастлабки концепциялардан воз кечиб, унинг янги тизимига ўтишни таклиф этмоқда.

Янги моделнинг асосий моҳияти тармоқдан фойдаланувчиларнинг анонимлигидан воз кечишдир. Бу тармоқнинг жиноий тажовузлардан янада кўпроқ ҳимояланган бўлишини таьминлашга имкон беради. Мисол тариқасида, ёпиқ тармоқ тизимига ўтган Хитой давлатини ва бундай жараёнга тайёргарлик кўраётган Россия давлатини келтиришимиз мумкин.

Жаҳон ҳамжамиятига интеграциялашаётган мамлакатимизда ахборот коммуникация технологиялари, ахборот тизимлари ва замонавий компьютер

технологияларидан самарали фойдаланиш бўйича изчил давлат сиёсати олиб борилмоқда.

Бугунги кунда мамлакатимизда жорий этилаётган замонавий рақамли технологиялар, фуқароларимизга қатор қулайликлар ва имкониятлар эшигини очмоқда.

Мазкур жараён билан бир қаторда, яратилаётган рақамли технологиялар ва ахборот тизимларининг хавфсизлигини таъминлаш муаммоси ҳам мавжуд, албатта.

Бу энг долзарб масалалардан бири - киберхавфсизликни таъминлаш, содир этилиши мумкин бўлган кибержиноятларнинг олдини олиш ва унга қарши курашишнинг энг зарур масаласи ҳисобланади.

Бизнингча, кундан-кунга такомиллашиб кетаётган кибержиноятчиликка қарши киберхавфсизликни таъминлашда қуйидаги асосий талабларни бажариш орқали улардан ҳимояланиш, яъни киберхавфсизликни таъминлашимиз мумкин бўлади:

- ходимларга (фуқароларга) ахборот хавфсизлиги асосларини ўргатиш;
- кибертахдидлар ҳақида огоҳликни ошириш мақсадида тушунтириш, огоҳлантириш бўйича ташвиқот тарғибот ишларини оммавий ахборот воситаларида кенг йўлга қўйилиши;
- фойдаланаётган дастурий маҳсулотларнинг заифликларини доимий синовдан ўтказиб бориш;
- ишончли антивирус дастурларидан фойдаланиш;
- лицензияланган расмий дастурлардан фойдаланиш;
- ахборот тизимларини ҳимоялашда кўп факторли аутентификациядан фойдаланиш;
- пароллардан фойдаланишда кучли паролни сақлаш сиёсатига риоя қилиш шунингдек, паролларни даврий равишда кучли паролларга алмаштириб бориш тартибига риоя қилиш;
- мунтазам равишда компьютер қаттиқ дискларидаги маълумотларни шифрлаш.
- махфий маълумотларнинг хакерлар қўлига тушиш ҳолати кўпинча корхона ташкилот идоранинг собиқ ходимлар билан боғлиқ бўлади. Шунингдек, заиф веб-сайтлар, айниқса онлайн тўлов ҳамда тизимлар ўрнатилган сайтларда кучли ҳимоялаш чораларини кўриши зарур.

Юқоридагилардан келиб чиқиб шуни таъкидлаш мумкинки, ахборот технологиялари соҳасидаги жиноятлар бўйича амалдаги жиноят кодексининг вазифалари шахсни, унинг ҳуқуқ ва эркинликларини, жамият ва давлат манфаатларини, мулкни, табиий муҳитни, тинчликни, инсоният хавфсизлигини жиноий тажовузлардан қўриқлаш, шунингдек жиноятларнинг олдини олиш, фуқароларни республика Конституцияси ва қонунларига риоя қилиш руҳида тарбиялашдан иборатдир.

Ана шу вазифаларни амалга ошириш учун жиноят кодекси жавобгарликнинг асослари ва принципларини, қандай ижтимоий хавфли қилмишлар жиноят эканлигини аниқлайди, ижтимоий хавфли қилмишлар содир

этган шахсларга нисбатан қўлланилиши мумкин бўлган жазо ва бошқа ҳуқуқий таъсир чораларини белгилайди.

Фойдаланилган адабиётлар рўйхати

1. Ўзбекистон Республикаси Конституцияси. (Янги таҳрирда) 2023 йил 30 апрель.
2. Ўзбекистон Республикасининг “Киберхавсизлик тўғрисида”ги ЎРҚ-764-сон қонуни. 2022 йил 15 апрель.
3. Ўзбекистон Республикасининг Жиноят кодекси. Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси. 1995. 1-сон.

КИБЕРЖИНОЯТЧИЛИК ВА УЛАРГА ҚАРШИ КУРАШИШНИНГ ЎЗИГА ХОС ЖИҲАТЛАРИ

З.Р.Умаров

ИИВ Малака ошириш институти Махсус касбий фанлар кафедраси профессори

Бугунги кунда яъни XXI асрда кибержиноятчилик аллақачон глобал муаммога айланиб улгурди деб айта оламиз. Барчамизга маълумки кибержиноятчиларнинг ҳаракатлари нафақат шахсларнинг шахсий маълумотлари, балки давлатларнинг хавфсизлиги, иқтисодий барқарорлиги ва фуқароларнинг ҳуқуқларини ҳам хавф остига қўямоқда. Кибержиноятчиликка қарши курашиш учун ҳуқуқий, ташкилий, молиявий-иқтисодий ва муҳандислик-техник жиҳатлардан комплекс чоралар кўриш лозимлигини тақозо қилмоқда.

Ҳозирги кунда ахборот-коммуникация технологияларидан кенг фойдаланган ҳолда ижтимоий алоқаларнинг ривожланиши глобал характерга эга бўлиб бормоқда. Бугунги кунда шундай технологиялар яратилмоқдаки, улар ёрдамида кишиларимиз ҳаётида катта қулайликлар яратилмоқда, товарлар сотиб олинмоқда, турли хизматлардан фойдаланмоқда, пул жўнатиш ва кабул қилиш, фуқароларимиз бир-бирлари билан мулоқот қилмоқда ҳамда маълумотлар алмашиш имкониятлари кенгаймоқда.

Жамиятимиз ривожланишининг устувор йўналишлари сифатида белгиланган ахборот технологиялари, телекоммуникация, маълумотларни узатиш тармоқлари, интернет хизматларидан фойдаланиш кенгаймоқда ва модернизациялашмоқда. Бугунги кунда белгиланган тадбирларни амалга оширилиши миллий ахборот тизимлари, ресурсларини яратишни, жамиятимиз ҳар бир аъзоси ҳаётига ва иқтисодиётга компьютер техникаси ва ахборот технологияларини оммавий жорий этилиши учун шароитлар яратилаётгани, жаҳон бозорида мамлакатимиз иқтисодиётининг рақобатбардошлигини оширади. Бинобарин ушбу муҳим қарорларни қабул қилинишига жамият ва

иқтисодиётни турли соҳаларида тезкор ахборот алмашинувига, дунё ахборот ресурсларидан фойдаланишга бўлган талаб, таълим жараёнларини ва инсонларнинг кундалик ҳаётини компьютерлаштириш зарурати ҳамда ахборот ва маълумотлар базаларининг хавфсизлигини таъминланиш талаби асос бўлиб хизмат қилмоқда.

Мамлакатимизда жадал олиб борилаётган ижтимоий-иқтисодий соҳадаги ислоҳотлар натижасида миллий иқтисодиёт ривожланмоқда, фуқароларимизнинг давлат органларига бўлган ишончини таборо ортиб боришини таъминлаш йўлида катта ўзгаришлар амалга оширилмоқда.

Аммо ўзининг кенг қамровлилиги билан ажралиб турувчи ахборот технологиялари соҳасида содир этилаётган фирибгарлик жиноятлари мамлакатимиз ҳаётида ўтказилаётган ислоҳотларга жуда катта зарар келтирмоқда. Шу ўринда мазкур жиноятларнинг содир этилиш усулига қарасак, уларнинг аксарияти ахборот технологиялари ва коммуникациялари орқали содир этилган ёки улар орқали жиноят содир этилиши учун имконият ҳамда шарт-шароит яратилган. Мисол тариқасида келтириш мумкинки, биткоинлар билан муаммо, интернет оламидан келадиган бой бўлишни хоҳлайсизми деган реклама кўринишидаги аслида хийла ва найрангни ўз ичига олган тузоқлар ҳаётимизда кўплаб учрамоқда.

Бугунги кунда бу фирибгарликнинг замонавий кўринишларидан бири киберфирибгарлик ёки интернет фирибгарлиги деб юритилмоқда, ушбу фирибгарлик тушунчаси Ўзбекистон Республикаси қонунчилигида, фақатгина Ўзбекистон Республикаси ЖКнинг 168-моддаси учинчи қисми “г” бандига асосан ахборот тизимидан, шу жумладан ахборот технологияларидан фойдаланиб содир этилган фирибгарлик жиноятларини содир этганлик учун жиноий жавобгарлик белгилаб қўйилган.

Ахборот технологиялари соҳасидаги ушбу ўзгаришлар мамлакатимиз фуқароларини ҳаёт сифатини яхшилаш билан бир қаторда, жиноятчиликнинг янги шакли сифатида интернет тармоқлари орқали содир этилаётган жиноят турларининг юзага келишига замин яратди ҳамда ҳаётимизга “кибержиноятчилик” тушунчасини олиб кирди. Бу эса ўз навбатида, инсонларни интернет ҳамлаларидан ҳимоялаш, ахборот олиш ва тарқатиш маданиятини тарғиб қилиш, тармоқ хавфсизлигини таъминлаш масалаларига ҳам жиддий эътибор қаратиш заруратини юзага келтирмоқда.

Интернет билан боғлиқ хавфсизликни таъминлаш бўйича халқаро Symantec Security ташкилотининг маълумотларига кўра, ҳозирда ҳар сонияда дунёдаги 12 нафар инсондан биттаси интернет ҳужуми қурбони бўлмоқда ва ҳар

йили 556 млн. дан кўпроқ киберҳужум уюштирилади ва бунда жабрланувчилар кўрадиган зарар миқдори 100 млрд. АҚШ долларидан кўпроқдир[68].

Дунёда «Глобал ахборотлаштириш ва компьютерлаштириш асри»да инсоният ҳаётида жахоншумул ихтироларни яратилиши билан бир қаторда, ахборот хавфсизлигига тобора таҳдиди ошиб бораётган интернет тармоқларидан фойдаланиб содир этилган жиноятларнинг тезкор тактик ва криминалистик жиҳатларини чуқур ўрганиш ҳамда таҳлил қилиш орқали, уларнинг содир этилиш усули ва воситаларига эътибор қаратган ҳолда тегишли куч ва воситлардан самарали фойдаланиш бўйича аниқ чора тадбирларни белгилаб олиш ва шу орқали содир этилган жиноятларни қисқа фурсатларда фош этиш юзасидан зарур таклиф ва тавсияларни ишлаб чиқиш бугунги ҳаётимизнинг долзарб масалаларига айланиб бормоқда.

Ўзбекистон Республикаси Президенти Шавкат Мирзиёев Шанхай ҳамкорлик ташкилотига аъзо давлатлар раҳбарлари кенгашининг мажлисида таъкидлаганидек, “кўп жиҳатдан аллақачон замонавий ҳаётни белгилаётган хавфсиз ахборот-коммуникация технологияларини ривожлантириш масалаларига ҳам эътибор қаратишни истар эдим.

Фақат кучларни бирлаштириш орқали, бир пайтнинг ўзида, ахборот маконидаги таҳдидларни камайтира борган тақдирдагина биз рақамлаштириш афзалликларидан тўла фойдалана олишимиз мумкин.

Кибержиноятчиликка қарши курашиш учун қўшма платформани яратиш вазифаси тобора долзарб бўлиб бормоқда[69].

Бугунги кунда мамлакатимизда интернетдан фойдаланувчилар сони 31 миллиондан ошиб бормоқда ва интернет тармоғига кирувчиларнинг аксарият қисми асосан мобил телефонлар орқали киришмоқда. Интернет тармоғидан фойдаланувчилар сонининг ортиши ва хизмат турлари кўпайиб бориши билан бирга кундалик ҳаётимизда кибержиноятчилик билан боғлиқ жиноятларни сони хам ортиб бормоқда. Ҳозирда республикамизда кибержиноятчиликнинг қуйидаги турлари нисбатан кўп содир этилаётганлиги маълум Жумладан:

---

[68]А.Анорбоев, Р.Хурсанов. Кибержиноятлар хавфини бартараф этиш йўллари. Илмий мақола. ОДИЛ СУДЛОВ. Ҳуқуқий, илмий-амалий нашр. 5/2020. 25-27 бетлар. https://sud.uz/wp-content/uploads /2021/odilsudlov/ 5_uz.pdf.

[69] Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг Шанхай ҳамкорлик ташкилотига аъзо давлатлар раҳбарлари кенгашининг мажлисидаги нутқи. // https://president.uz/uz/lists/view/5542 (16.09.2022 й.)

- интернет фойдаланувчиларнинг шахсий (махфий) маълумотларини эгаллаш ва уларни ошкор қилиш билан қўрқитиб товламачилик қилиши (кибертовламачилик);

- фирибгарлар фойдаланувчилар телефонига хар-хил танлов ғолиби бўлганлиги ҳақидаги хабарни юбориб, уларнинг банк карталари билан боғлиқ бир марталик юборилган SMS-кодни, тижорат банклари, тўлов тизими операторлари ва тўлов ташкилотларининг мобил иловаларига кириш ҳуқуқини берувчи логин ва паролларни эгаллаб, пластик картасидага маблағларни ўзлаштириши;

- Охирги вақтларда авж олаётган фирибгарлик турларидан яна бири – Telegram гуруҳларга одам қўшиш орқали қанчадир маблағ билан тақдирланишдир. Ушбу ҳолатда ҳам фирибгарлар телефон рақам ва пластик карта маълумотларини билиб олиб, ҳисобдан пул ечиб олиши;.

- ижтимоий тармоқда зўрлик ишлатиш билан қўрқитиши, ҳақорат, суицид ҳолатлари (кибербуллинг) ва бошқалар .

Юқорида келтирилган фирибгарликларни олдини олиш ва уларга қарши курашиш мақсадида мамлакатимизда олиб борилаётган рақамли иқтисодиётга оид ислоҳотларнинг самарадорлигини ошириш ҳамда фуқароларимизнинг ахборот технологиялари соҳасидаги билимлари даражасини оширилиши мухимдир. Бу борада ишларимизни янада жадаллаштиришимиз халқимизнинг ахборот технологияларига нисбатан ишончи ҳамда онгининг ортиб боришига хизмат қилади. Мамлакатимизда амалга оширилаётган суд-ҳуқуқ тизимидаги ислоҳотлардан кўзланган асосий мақсад ҳам жамиятда тинчлик ва осойишталикни сақлаш, жамоат тартиби ҳамда хавфсизлигини таъминлаш, фуқароларнинг ҳуқуқ, эркинликларини ҳар қандай кўринишдаги тажовузлардан ҳимоя қилишдир.

Ахборот технологияларидан фойдаланиб содир этилаётган фирибгарлик жиноятларига қарши курашиш самарадорлигини оширишга мақсадида, банк пластик карталари ва интернет хизматлари орқали содир этилган ҳар бир пул ўғирлаш ва фирибгарлик ҳолатлари бўйича олиб борилаётган дастлабки суриштириув ҳаракатлари юзасидан тез фурсатда қонуний қарор қабул қилинишини таъминлаш мақсадида, Ички ишлар вазирлиги билан Марказий Банк, процессинг марказлари (uzcard, humo), интернет тўлов тизими иловалари (payme, paynet, clik, apelsin, ва ҳ.к) марказлари билан самарали ҳамкорлик механизмларини йўлга қўйиш мақсадга мувофиқ бўлади. Бундан ташқари банк пластик карталаридан фирибгарлик орқали пул маблағларини талон-тарож қилинишининг олдини олиш мақсадида мижозлар томонидан ўзларига тегишли

бўлган банк пластик карталарини турли иловаларга улаш ва фаоллаштиришда “Face-ID” тизимидан фойдаланишни киритиш билан ахборот технологияларидан фойдаланиб содир этилаётган турли фирибгарликлардан фуқароларимизни ҳимоялаган бўламиз.

Бугунги кунда ахборот технологиялари орқали содир этилган ҳуқуқбузарлик ҳолатлари юзасидан келиб тушган ҳар бир мурожаатларни текширув натижаси бўйича унинг қонунийлиги ва жазо муқаррарлигини таъминлаш мақсадида, Ўзбекистон Республикаси ИИВ тизимида Республика миқёсида ушбу турдаги жиноятларни содир этиб келаётган ҳамда жиноятларни содир этишга мойил шахсларни рўйхатининг ягона базасини шакллантириш ва бу борада маълумотлар алмашинуви билан боғлиқ тезкор ишларни амалга оширилиши мухим вазифалардан бир бўлиб ҳисобланади.

Ахборот технологиялари орқали содир этиладиган ҳуқуқбузарликларга қарши курашиш ваколатига эга давлат органлари, жумладан, Ички ишлар органлари ходимларининг кибержиноятчиликка қарши кураш ва ахборот технологияларидан фойдаланиб содир этилган фирибгарликлар бўйича билим ва кўникмаларини мунтазам равишда такомиллаштириб бориш юзасидан чора тадбирларни белгилаб олиниши зарур.

Мухтасар қилиб айтганда, ахборот технологияларидан фойдаланиб содир этилган фирибгарлик жиноятларини аниқлаш, олдини олиш, қарши курашиш ва уни бартараф этиш бўйича зарур қарорлар қабул қилиш, кибержиноятчиликка қарши курашиш бўйича норматив-ҳуқуқий ҳужжатлар лойиҳаларини ишлаб чиқишда иштирок этиш, давлат органлари ва халқ манфаатларига таҳдид солувчи киберхатарларни аниқлаш ва уларга қарши курашиш, фуқароларнинг ҳуқуқ ва эркинликларига таҳдид солувчи кибержиноятларнинг содир этилишига имкон яратувчи сабабларни бартараф этиш каби муҳим вазифаларни бажариш ҳам бугунги куннинг долзарб масалаларидан бири эканлигини унутмаслик лозим. Бинобарин, мамлакатимиздаги ҳар бир фуқаронинг хавфсизлигини таъминлаш энг муҳим масалалардан бири хисобланади.

Фойдаланилган адабиётлар:

1.O‘zbekiston Respublikasining Qonuni Kiberxavfsizlik to‘g‘risida https://lex.uz/uz/docs/5960604 (Qonunchilik ma’lumotlari milliy bazasi, 16.04.2022 y., 03/22/764/0313-son)
2.https://oltinsoy.uz/oz/blog/ududij-b-limlar/253

KIBERXAVFSIZLIKNING IIODAGI AHAMIYATI

Xojibekov Ziyomiddin Nasriddinovich

Kasbiy tayyorgarlik fakulteti Maxsus fanlar sikli katta o‘qituvchisi

Dunyo miqiyosida axborot texnologiyalarining rivojlanishi, XXI asr – axborot texnologiyalar asri bo‘lganligi, insonlarga qanchalik qulay bo‘lgan bo‘lsa, shunchalik ularning hayoti va shaxsiy ma’lumotlariga bo‘lgan xafvsizlikning kamayishiga olib keldi. Insonlar o‘rtasida elektron pullar ishlatilib ularning qancha qulayligi ortgan bo‘lsa, ularga nisbatan hujum ham shu darajada ortdi. Aynan ushbu sohalardagi xafvsizlik “Kiberxafvsizlik” bilan ta’minlanadi.

Kibermakonda sodir bo‘layotgan jinoyatlar soni hozirgi kunga sezilarli darajada oshdi. Kibermakondagi jinoyatlarning boshqa jinoyatlardan farqi bu jinoyatni shaxs masofadan sodir qiladi, inson bu jinoyatni o‘z ko‘zi bilan ko‘rmaydi, bu jinoyatda inson hayotiga emas balki ma’lumotlariga hujum bo‘ladi. Shuning uchun bu kabi jinoyatlarga qarshi kurashish uchun mamlakatda samarali ish olib boruvchi organlar tizimini yaratishni taqazo qiladi.

O‘zbekiston Respublikasida kiberxavfsizlik sohasidagi munosabatlarni tartibga solish, kiberjinoyatlarni oldini olish, kiberhujumdan himoyalanish maqsadida Oliy Majlis tomonidan 15.04.2022 yil sanasida “Kiberxafvsizlik to‘g‘risida”gi O‘zbekiston Respublikasi qonuni qabul qilindi va 17.07.2022 yil sanasidan kuchga kirdi.

Qabul qilingan qonunda kiberxafvsizlik sohasidagi muhum tushunchalarning to‘liq ma’nolari ochib berildi. Qonunda kiberxafvsizlik sohasidagi munosalatlarni o‘z prinsplari orqali tartibga solish belgilandi. Bu prinsiplarni

qonuniylik;

kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi;

kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv;

kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;

O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi kabi prinsiplar tashkil qiladi.

O‘zbekiston Respublikasida kiberxavfsizlik sohasidagi yagona davlat siyosatini O‘zbekiston Respublikasi Prezidenti belgilaydi.

O‘zbekiston Respublikasi Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organidir. O‘zbekiston Respublikasi Davlat xavfsizlik xizmatiga kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlarni va davlat dasturlarini ishlab chiqishi, kiberxavfsizlik to‘g‘risidagi qonunchilik hujjatlarining ijro etilishi ustidan nazoratni amalga oshirishi, kiberxavfsizlik hodisalari yuzasidan tezkor-qidiruv tadbirlarini, tergovga qadar tekshiruvlarni va tergov harakatlarini amalga oshirish, kiberxavfsizlik hodisalarining oldini olish, ularni aniqlash va bartaraf etish hamda ularga nisbatan tegishli chora-tadbirlarni, shu jumladan ularning oqibatlarini tugatish bo‘yicha tashkiliy-texnik chora-tadbirlarni ko‘rishi, favqulodda vaziyatlarda axborot tizimlari va resurslarini kiberhimoya qilish hamda kiberxavfsizlik sohasidagi boshqa masalalar bo‘yicha chora-tadbirlarni o‘z ichiga olgan rejalarni ishlab chiqishi,

kiberxavfsizlikni ta’minlashga doir ishlarni, shuningdek muhim axborot infratuzilmasi obektlarida kiberhujumlarning oldini olishga, ularni aniqlashga va ularning oqibatlarini tugatishga doir ishlarni tashkil etishi, muhim axborot infratuzilmasi obektlarining kiberxavfsizligini ta’minlashga doir talablarni belgilashi kabi bir qancha yangi vazifalar yuklatildi.

Kiberxavfsizlik hozirgi vaqtda jamiyat va iqtisodiyotning har bir sohasida muhim ahamiyatga ega. Rakamli texnologiyalar, internet va internet-qarorlaridan foydalanish jamiyatning barcha tarmoqlarini qamrab olgani sari, kiber xavfsizlik masalalari ham kundan-kunga aniqroq bo‘lib, kiber jinoyatlar va tahdidlarga qarshi choralarni ishlab chiqish va amalga oshirish talab etilmoqda.

Kiberxavfsizlikning jamiyatdagi ahamiyati:

-shaxsiy ma’lumotlarni himoya qilish bunda raqamli jamiyatda shaxsiy ma’lumotlar (pasport ma’lumotlari, bank kartalari, to‘lov ma’lumotlari, internet bank axboroti) internet orqali safarbar qilinadi, tarqatiladi va saqlanadi. Kiber hujumlar va ma’lumotlar ustidagi xavflar, shaxsiy ma’lumotlarning o‘g‘irlanishiga olib kelishi mumkin. Buning natijasida fuqarolarning moliyaviy manfaatlari va shaxsiy xavfsizligiga katta zarar yetkazilishi mumkin.

Qonun buzish va kiber jinoyatlar, kiberxavfsizlikning muhim jihatlaridan biri internetdagi qonunbuzarliklar, jinoyatlar va xakerlik ishlariga qarshi kurashishdir. Internet orqali turli xil shaxsiy, moliyaviy va davlat axborotlari o‘g‘irlanishi, firibgarlik, virtual terrorizm va xakerlik xurujlari jamiyatga xavf soladi. Kiber xavfsizlik ushbu xavflarni aniqlash, ularga qarshi reaksiya va profilaktika choralarini amalga oshirish uchun muhimdir:

- korxonalar va bizneslarning xavfsizligi tijorat va korporativ dunyoda raqamli texnologiyalar va internet xizmatlari muhim rol o‘ynaydi. Elektron tijorat, onlayn bank xizmati, raqamli reklama va turli xil biznes-hizmatlar kiberxavfsizlikka jiddiy xavf tug‘diradi. Korxonalar uchun o‘z biznesi va mijozlarining ma’lumotlarini muhofaza qilish muhim ahamiyatga ega. Kiber hujumlar, shaxsiy ma’lumotlarni olish yoki ishlab chiqarish jarayonlarini to‘xtatish orqali biznesdagi moliyaviy zarar va noma’lum iqtisodiy oqibatlar bo‘lishi mumkin.

-internet orqali ma’lumotlarni tarqatish va axborot manipulyatsiyasi internet orqali axborot tarqatish bilan bog‘liq xavflar ham kundan-kunga ortib bormoqda. Yolg‘on axborotlar (fake news) va manipulyatsiyalar jamiyatdagi muhokamalarga ta’sir qiladi, shunday qilib, internet orqali axborot xavfsizligini ta’minlash jamiyatdagi tinchlik va barqarorlikka xizmat qiladi.

-fuqarolarning onlayning xavfsizligini ta’minlash har bir fuqaro internetdan foydalanganda kiberxavfsizlikni o‘rganishi kerak. Virtual xavfsizlikni ta’minlash uchun maxfiy parollar, viruslarga qarshi muhofaza qilish va internetdagi xavfsizlik to‘g‘risidagi bilimlarni oshirish muhimdir. Odamlar shaxsiy ma’lumotlarni, qarzlarini, omonatlarini va boshqa moliyaviy resurslarini muhofaza qilishda ehtiyot bo‘lishi kerak.

Hozirgi vaqtda mamlakatimizda, Ichki ishlar organlari tizimida kiberxavfsizlikning ahamiyati muhim va dolzarb masalaga aylandi. Raqamli texnologiyalar va internetning hayotimizga keng kirib kelishi bilan ichki ishlar organlari ham kiber xurujlar, internetdagi jinoyatlar va ma’lumotlar xavfsizligini

ta’minlash kabi yangi muammolarga duch kelmoqda. Buni hisobga olgan holda, ichki ishlar organlarida kiberxavfsizlikning o‘rni va ahamiyati yanada kuchaytirilmoqda.

Jamiyatda rivojlanayotgan kiber jinoyatlar — bu internet orqali amalga oshiriladigan jinoyatlar, shu jumladan, internet firibgarligi, shaxsiy ma’lumotlarni olish (hakerlik), virtual terrorizm, onlayn shantaj, va turli xil ko‘rsatkichlar yoki elektron hujjatlarni taqlid qilish kabi holatlarni qamrab oladi.

Shuningdek IIO ma’lumotlarni himoya qilish, axborotlar tizimini muhofaza qilish va xavfsizlikni ta’minlash vazifasini bajarishi kerak. Bu, jumladan, jinoyatchilardan, jamoat tashkilotlari va davlat xizmatlaridan olingan ma’lumotlarni xavfsiz saqlashni o‘z ichiga oladi. Shuningdek, ichki ishlar organlari o‘z ma’lumotlarini xakerlik hujumlaridan, viruslardan va boshqa kiber xavflardan himoya qilish uchun yuqori darajadagi xavfsizlik choralarini ishlab chiqishi lozim.

IIOning kiberxavfsizlikni ta’minlashdagi rollaridan yana biri bu davlat organlari va fuqarolar o‘rtasidagi aloqa kanallarini muhofaza qilishdir. Masalan, onlayn arizalar, pasportlarning elektron shaxsni tasdiqlash, ijara shartnomalari va boshqa yuridik hujjatlar jamiyatda kundalik hayotning bir qismiga aylangan. Buning uchun ichki ishlar organlari elektron xujjat aylanishini muhofaza qilish va internet orqali xizmat ko‘rsatish tizimlarining xavfsizligini ta’minlashda ishtirok etishi lozim.

Xulosa sifatida kiberxavfsizlik jamiyatdagi har bir sohaga taalluqli bo‘lib, zamonaviy raqamli jamiyatning asl bo‘g‘inidir. Bu, faqat shaxsiy yoki korxona xavfsizligi bilan cheklanmay, butun davlat va global xavfsizlikning barqarorligini ta’minlaydi. Raqamli dunyoda ishlash va rivojlanishda kiber xavfsizlikka jiddiy e’tibor qaratish hamjamiyatni xavflardan himoya qilish, samarali faoliyat ko‘rsatish va tinchlikni saqlash uchun muhim ahamiyatga ega.

Foydalanilgan adabiyotlar:

1.O‘zbekiston Respublikasining Qonuni Kiberxavfsizlik to‘g‘risida https://lex.uz/uz/docs/5960604 (Qonunchilik ma’lumotlari milliy bazasi, 16.04.2022 y., 03/22/764/0313-son)
2.https://oltinsoy.uz/oz/blog/ududij-b-limlar/253

ҲАРБИЙ ХИЗМАТЧИЛАРНИНГ ВИРТУАЛ РЕАЛЛИК ТЕХНОЛОГИЯЛАРИДАН ФОЙДАЛАНИШ ИСТИҚБОЛЛАРИ

Иргашев Даврон Рустамович

Мудофаа вазирлиги ҳузуридаги Мудофаа саноати агентлиги бош мутахассиси

Аннотация: Ушбу мақолада ҳарбий соҳада виртуал реаллик технологияларининг қўлланилиши ва уларнинг самарадорлигини оширишга қаратилган алгоритмларни таҳлил қилиш, виртуал реаллик технологиялари ёрдамида жанговар тайёргарлик, стратегик режалаштиришдаги аҳамияти, шунингдек, технологияни самарали қўллаш учун зарур бўлган алгоритмик ёндашувлар кўриб чиқилади.

Калит сўзлар: Виртуал реаллик, алгоритм, виртуал миҳит, сунъий интеллект экстремал вазиятлар, жанговар тайёргарлик, симуляция ва тренажёрлар, виртуал муҳит, моделлаштириш ва симуляция, 3D моделлар.

VR технологиялари ҳарбий хизматчиларга ҳақиқий жанговар шароитларга ўхшаш симуляцияларда ўқув машғулотларини ўтказиш имконини бериш билан бир қаторда уларнинг жанговар тайёргарлигини ошириш, хавфсизлик ва самарадорликни кучайтиришга хизмат қилади.

VR технологияси ҳарбий таълим ва тайёргарлик жараёнини тубдан ўзгартириш салоҳиятига эга бўлиб, ҳарбий хизматчиларга жанговар шароитларни хавфсиз ва самарали тарзда тажриба қилиш имкониятини яратиди. VR ёрдамида ҳарбий хизматчиларнинг реал жанговар вазиятларга ўхшаш муҳитда, жанговар тактика ва стратегияларни ўрганиш ҳамда мураккаб вазиятларда қарор қабул қилиш малакасини ривожлантиришга қаратилган.

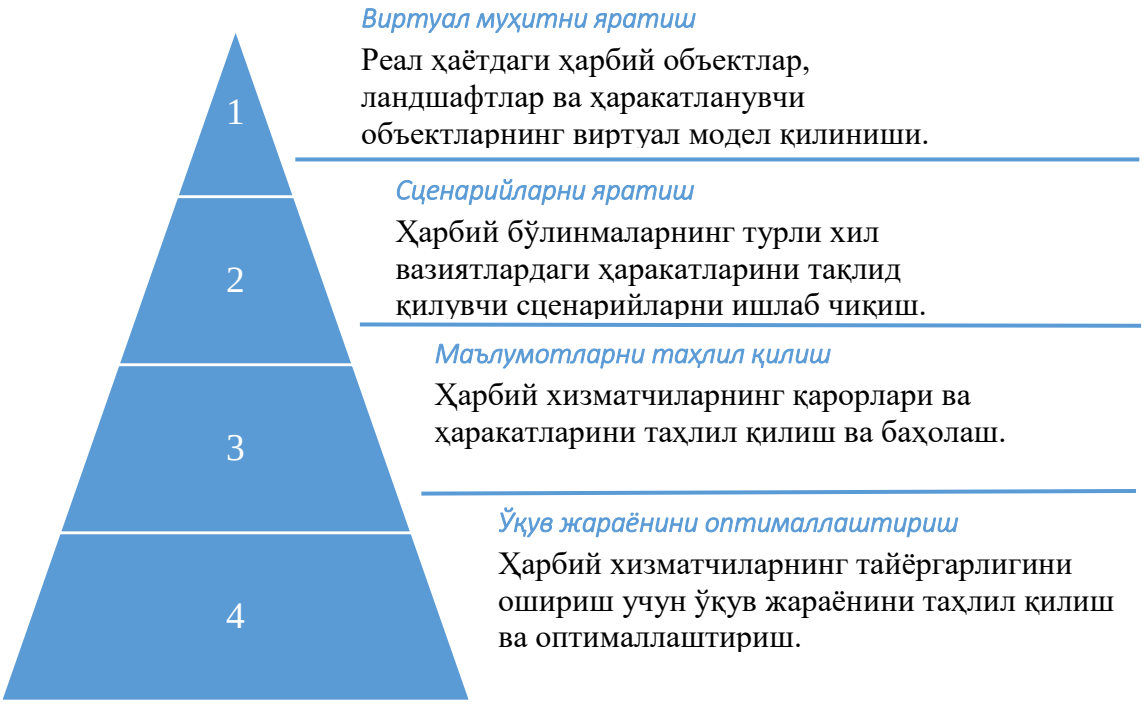
VR технологиялари ҳарбий хизматчиларга жанговар шароитларда қўлланиладиган турли хил қуроллар ва техникалар билан ишлаш имконияти, уларга турли хил ҳужум ва мудофаа тактикаларини ўргатиш, шунингдек, жанг майдонида ҳаракатланиш ва қутқарув операцияларда ҳамда жанговар вазиятларда ҳаракатланиш қоидалари, шунингдек, экстремал шароитларда ҳаётни сақлаб қолиш усулларини бир неча маротаба машқларни ўзлаштириш имкониятилар мавжуд.

Шу билан бирга VR технологиялари хавфсизликни ошириш ҳарбий хизматчиларни реал жанговар вазиятларга тайёргарлик кўришда ҳарбий хизматчиларнинг хавфсизлигини ошириш ва жанговар йўқотишларни камайтиришга имкон мавжуд.

Шунингдек, VR технологиялари ёрдамида ҳарбий хизматчилар ўзларининг жанговар тайёргарлик даражасини баҳолашлари ва камчиликларни аниқлашлари ҳамда бартараф этиш чораларини машқ қилишлари мумкин.

Экстремал вазиятларни тақлид қилиш ва моделлаштириш усуллари

Виртуал реаллик технологиялари ёрдамида ҳарбий бўлинмаларни тайёрлашда экстремал вазиятларни тақлид қилиш ва моделлаштириш муҳим аҳамиятга эга. Бу эса ҳарбий хизматчиларга ҳақиқий жанг шароитида ўхшаш муҳитда ҳаракат қилишни, тўғри қарорлар қабул қилиш имконини беради.



Виртуал реаллик технологияларидан фойдаланган ҳолда турли хил экстремал вазиятлар, жумладан, жанг майдонидаги ҳужум ва ҳимоя ҳаракатлари, террорчилик ҳужумлари, табиий офатлар ва бошқа экстремал вазиятларни тақлид қилиш мумкин. Бу ҳарбий хизматчиларга ҳақиқий ҳаётдаги ҳаракатларнинг натижаларини кузатиб, хатолардан сабоқ олиш ва ўзларининг ҳаракатларини такомиллаштириш имконини яратади.

Виртуал реаллик технологияларидан фойдаланган ҳолда ҳарбий кучларни тайёрлашнинг хусусиятлари

Виртуал реаллик технологиялари ҳарбий тайёргарликда анъанавий усулларни тўлдириш ва такомиллаштириш имконини беради. Бу эса виртуал реаллик технологиялари ҳарбий хизматчиларни амалий отиш машқларига нисбатан хавфсиз ва самарали муҳитда экстремал вазиятларга тайёрлаш имконини беради. VR технологияларининг ҳарбий тайёргарликда қўлланилишининг асосий хусусиятлари қуйидагилар:

- **реал вақтдаги тажриба:** VR технологиялари ҳарбий хизматчиларни ҳақиқий жанговар вазиятларга ўхшаш тажрибага эга бўлиш;
- **хавфсизлик ва самарадорлик:** VR технологиялари ҳарбий хизматчиларни хавфли вазиятларга тушишдан ҳимоя қилади ва шу билан бирга, тайёргарлик жараёнини тезлаштириш ва самарадорлигини ошириш;
- **қайта-қайта машқ қилиш имконияти:** VR технологиялари ҳарбий хизматчилар бир неча маротаба бўлса ҳам машқ қилиши ва хатоларидан сабоқ олиш;
- **мос шарт-шароитларни яратиш:** VR технологиялари ҳар қандай жанговар вазиятларни, жумладан, душман ҳаракатлари, ҳаво ҳужуми, табиий офатлар ва бошқа вазиятларни симуляция қилиш.

VR технологиялари ҳарбий хизматчиларни хавфсиз ва самарали муҳитда жанговар тайёргарликка, тактик ҳаракатларга ва жамоавий ҳамкорликка тайёрлашга имкон беради. Шу билан бирга, VR технологиялари ҳарбий

хизматчиларнинг стрессга чидамлилигини, қарор қабул қилиш қобилиятини ва жанговар руҳий тайёргарлигини оширишга ёрдам беради.

Шунингдек, виртуал реаллик технологиялари ёрдамида командир ва бошлиқларни тайёрлашда муҳим роль ўйнайди. Мазкур технология ёрдамида турли хил вазиятларни, жумладан, жанговар ҳаракатларни, табиий офатларни ва бошқа экстремал ҳолатларни симуляция қилиш имкониятига эга бўладилар. VR технологиялари ҳарбий хизматчиларнинг тактик ва стратегик фикрлаш қобилиятини ошириш, муаммоларни тез ва самарали ҳал қилиш, шунингдек, жамоавий ҳаракатларини мувофиқлаштиришга ёрдам беради.

VR технологияларида командир ва бошлиқлар турли хил вазиятларда, масалан, душман ҳужуми остида ёки табиий офатлар пайтида қандай ҳаракат қилишларини, қўшинларни бошқариш, ресурсларни тақсимлаш, ахборотни таҳлил қилиш ва қарорлар қабул қилишни ўрганадилар.

Шунингдек:

VR ёрдамида ҳарбий хизматчилар турли хил жанговар ҳаракатларга тайёргарлик кўриш;

VR технологияларида ҳарбий хизматчилар турли хил машқларни, масалан, жанговар ҳаракатларни, табиий офатларни ва бошқа экстремал ҳолатларни симуляция қилиш;

VR технологиялари ҳарбий хизматчиларнинг тактик ва стратегик фикрлаш қобилиятини ошириш, муаммоларни тез ва самарали ҳал қилиш, шунингдек, жамоавий ҳаракатларни мувофиқлаштиришга ёрдам беради.

Ҳарбий тайёргарлик жараёнида виртуал реаллик технологияларининг қўлланиши билан боғлиқ хавфсизлик масалалари

Ҳарбий тайёргарликда виртуал реаллик технологияларининг қўлланилиши кўплаб фойдалар билан бирга, баъзи хавфсизлик масалаларини ҳам ўз ичига олади. Масалан, симуляция қилинаётган муҳитларни ҳаддан ташқари ҳақиқий тасвирлаш, ўйинчиларнинг виртуал дунёга шошилганлиги, ҳарбий тайёргарлик учун махфий маълумотларнинг хавфсизлиги ва VR тизимларининг техник хатолари каби масалалар кўриб чиқилади.

Виртуал реаллик технологияларининг ҳаддан ташқари ҳақиқий тасвирлаш муаммоси ҳарбий тайёргарликда ўйинчиларнинг психикасига салбий таъсир кўрсатиши мумкин. Масалан, жанг майдонидаги виртуал ҳаракатларни ҳаддан ташқари ҳақиқий ҳис қилиш, стресс ва психологик шикастланишга олиб келиши мумкин. Шунингдек, виртуал реаллик технологиялари ўйинчиларнинг виртуал дунёга шошилганлигига олиб келиши мумкин. Бу эса, уларнинг ҳақиқий дунёдаги муаммоларга тўғри жавоб бериш қобилиятига салбий таъсир кўрсатиши мумкин.

Ҳарбий тайёргарликда қўлланиладиган виртуал реаллик технологияларининг хавфсизлиги ҳам муҳим масала ҳисобланади. Масалан, симуляция қилинаётган муҳитларни ҳимоя қилиш, ҳарбий махфий маълумотларнинг хавфсизлигини таъминлаш ва виртуал реаллик тизимларининг хавфсизлигини кафолатлаш зарур.

VR тизимларининг техник хатолари ҳам ҳарбий тайёргарликда хавфсизлик масалаларини келтириб чиқариши мумкин. Масалан, симуляция қилинаётган

муҳитдаги техник хатолар, ўйинчиларнинг хавфсизлигига хавф туғдириши мумкин. Шунингдек, тизимнинг тўхтаб қолиши ёки ишламай қолиши ҳам ҳарбий тайёргарлик жараёнини бузиши мумкин.

Хулоса. Виртуал реаллик технологиялари ўзининг узоқ ва мураккаб тарихий йўлини босиб ўтди. Илк назарий ғоялардан то замонавий юқори технологияли қурилмаларгача бўлган бу йўл инсон тафаккури ва технологик тараққиётнинг ёрқин намунасидир.

Бугунги кунда ВР технологиялари нафақат кўнгилочар саноат, балки таълим, тиббиёт, бизнес ва бошқа кўплаб соҳаларда қўлланилмоқда. Келажакда эса бу технологиялар янада ривожланиб, инсон ҳаётининг ажралмас қисмига айланиши кутилмоқда. Шубҳасиз, виртуал реаллик инсоният олдида янги имкониятлар эшигини очмоқда, аммо у билан боғлиқ хавф ва муаммоларни ҳам эътибордан четда қолдирмаслик лозим.

KIBERJINOYATCHILIKKA QARSHI KURASHNING MUXANDISLIK-TEXNIK TA’MINOTI

Axmadxonov Afzaliddin Abduvosi o‘g‘li

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti magistratura tinglovchisi

Kirish. Kiberjinoyatchilik sohasidagi xavf-xatarlar har yili o‘sib bormoqda. Internet va raqamli texnologiyalarning rivojlanishi bilan kiberjinoyatlar ko‘paymoqda, va ular global miqyosda xavf tug‘diradi. Kiberjinoyatchilikka qarshi kurashishning samarali mexanizmlarini ishlab chiqish, shu jumladan, muxandislik-texnik ta’minotni rivojlantirish, bu masalalarni hal etishda muhim ahamiyatga ega.

Kiberjinoyatchilik va uning turlari

Kiberjinoyatchilik turli shakllarda namoyon bo‘ladi. Ular orasida quyidagi asosiy yo‘nalishlar ajratib ko‘rsatiladi:

Kiberhujumlar: Kompyuter tizimlari va tarmoqlariga ruxsatsiz kirish, ma’lumotlarni o‘g‘irlash yoki zararlash.

Phishing (fishing): Foydalanuvchilarning maxfiy ma’lumotlarini to‘plash maqsadida yolg‘on ma’lumotlar yuborish.

Ransomware (sezgir dasturlar): Ma’lumotlarni shifrlash va foydalanuvchidan pul talab qilish.

Hackerlar va botnetlar: Tarmoqlarda zararli faoliyatni amalga oshirgan foydalanuvchilar yoki tizimlar.

Muxandislik-texnik ta’minotning roli

Kiberjinoyatchilikka qarshi kurashda muxandislik va texnik ta’minotning o‘rni juda katta. Bunda quyidagi asosiy mexanizmlar ishlatiladi:

Kriptografiya: Ma’lumotlarning maxfiyligini ta’minlash, ularni o‘g‘irlashdan himoya qilish uchun kriptografik usullar (AES, RSA) va ochiq kalitli tizimlar ishlatiladi.

Tarmoq xavfsizligi: Kompyuter tarmoqlarining xavfsizligini ta’minlash uchun joriy etilgan vositalar (firewall, intrusion detection system (IDS), intrusion prevention system (IPS)).

Antivirus va zararlanuvchi dasturlarni aniqlash: Antivirus dasturlari va zararlanuvchi dasturlarni aniqlash va ularni bartaraf etish tizimlari kiberjinoyatchilikka qarshi kurashda samarali vositalardan biridir.

Biometrik xavfsizlik: Foydalanuvchining shaxsini tasdiqlash uchun biometrik tizimlardan foydalanish (otmish hujjatlari, barmoq izlari, yuzni aniqlash).

Yangi texnologiyalarning tatbiqi

Yangi texnologiyalar, ayniqsa sun'iy intellekt (SI) va mashina o'rganish, kiberjinoyatchilikka qarshi kurashishda samarali vositalar yaratmoqda. SI yordamida hujumlar va tarmoqdagi xavf-xatarlarni aniqlash imkoniyatlari oshmoqda.

Mashina o'rganish: Avtomatik tarzda anomal tarmoq faoliyatlarini aniqlash va kiberhujumlarni erta bosqichda aniqlash.

Blokcheyn texnologiyasi: Ma'lumotlar xavfsizligini ta'minlashda blokcheyn texnologiyasi va uning raqamli imzolar yordamida ma'lumotlarning o'zgartirilishini oldini olish.

Kiberjinoyatchilikka Qarshi Kurashishda Xalqaro Hamkorlik

Kiberjinoyatchilik transmilliy xususiyatga ega bo'lgani sababli, u bilan kurashishda xalqaro hamkorlik zarur. Bunday hamkorlik kiber jinoyatchilikka qarshi kurashishda qonunlar, texnologiyalar va resurslarni muvofiqlashtirishga yordam beradi. BMT va boshqa xalqaro tashkilotlar, shuningdek, o'zaro kelishuvlar va konferensiyalar orqali kiberjinoyatchilikka qarshi kurashishga doir bir nechta tashabbuslarni amalga oshirishmoqda.

Xulosa. Kiberjinoyatchilikka qarshi kurashishning muxandislik-texnik ta'minoti bugungi kunda eng muhim va dolzarb masalalardan biri hisoblanadi. Yangi texnologiyalar va ilg'or muhandislik yechimlari kiberjinoyatchilikka qarshi samarali vositalarni yaratishda yordam beradi. Shuningdek, xalqaro hamkorlik va davlatlararo kelishuvlar kiberjinoyatchilikka qarshi kurashishda muvaffaqiyatga erishishda katta rol o'ynaydi.

Adabiyotlar ro'yxati:

1. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
2. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.
3. Rainer, P. (2019). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.
4. Liu, J., & Zhang, Z. (2022). *Artificial Intelligence for Cybersecurity: Machine Learning Techniques and Applications*. Springer.
5. Gordon, L. A., & Loeb, M. P. (2021). "The Economics of Information Security: From Information Warfare to Cybercrime". *Journal of Computer Security*, 29(3), 361-379.
6. Mavroeidis, V. (2020). *Blockchain for Cybersecurity and Privacy Protection*. Wiley.

IJTIMOIY KOMPETENTLIKNI RIVOJLANTIRISHNING PSIXOLOGIK XUSUSIYATLARI VA KIBIR XAVFSIZLIGI: ZAMONAVIY JAMIYATDA SHAXSIY RIVOJLANISH VA XAVFSIZLIKNI TA'MINLASH

Qodirov Islombek Ravshanbek o'g'li

O'zbekiston Respublikasi Jamoat xavfsizligi universiteti magistratura tinglovchisi

KIRISH. Zamonaviy jamiyatda shaxsning ijtimoiy kompetentligi va kibir xavfsizligi o'rtasidagi o'zaro aloqalar har qanday ijtimoiy, psixologik va texnologik o'zgarishlarga qarshi turish va muvaffaqiyatli integratsiya qilishda muhim ahamiyat kasb etadi. Ijtimoiy kompetentlik, shaxsning jamiyatdagi muloqot va aloqalar jarayonida samarali ishlash qobiliyatini ifodalaydi, bu esa o'z navbatida ijtimoiy barqarorlik va shaxsiy xavfsizlikni ta'minlashga xizmat qiladi. Kiberya xavfsizligi esa onlayn muhitda shaxsiy ma'lumotlarning himoya qilinishini ta'minlashga qaratilgan strategiyalardan iborat. Ushbu tezisda ijtimoiy kompetentlikni rivojlantirish va kibir xavfsizligini ta'minlashning psixologik aspektlari tahlil qilinadi.

Ijtimoiy kompetentlik va uning psixologik xususiyatlari

Ijtimoiy kompetentlikni rivojlantirishning psixologik jihatlari:

Empatiya va muloqot qobiliyatlari: Ijtimoiy kompetentlik o'z ichiga empatiya, ya'ni boshqalar hissiyatini tushunish va ularga mos ravishda javob berish qobiliyatini oladi. Shaxslar o'rtasidagi muvaffaqiyatli aloqalar psixologik bexavotirlikni kamaytiradi va ijtimoiy xavfsizlikni ta'minlaydi. Empatiya muloqotda qabul qiluvchi va javob beruvchi tomonlarning o'zaro anglashuvini osonlashtiradi, bu esa jamiyatdagi o'zaro ishonchni kuchaytiradi.

Shaxsiy va ijtimoiy identifikatsiya: Ijtimoiy kompetentlik shaxsning o'zini jamiyatda qanday ko'rsatishini va qanday rolda faoliyat ko'rsatishini belgilaydi. Shaxsning o'ziga bo'lgan ishonchi va uning o'zini jamiyatda qanday qabul qilishi ham ijtimoiy kompetentlikni belgilovchi muhim psixologik omil hisoblanadi. Ijtimoiy identifikatsiya, ya'ni shaxsning o'zini guruh yoki jamiyat a'zosi sifatida qanday his qilishi, uning muloqotdagi muvaffaqiyatiga ta'sir ko'rsatadi. Bunday identifikatsiya ijtimoiy xavfsizlik va umumiy jamiyatdagi o'rnini anglashni ta'minlaydi.

Ijtimoiy qobiliyatlarni rivojlantirish: Ijtimoiy qobiliyatlar, jumladan, muloqot, hamkorlik va ijtimoiy vaziyatlarga moslashuv, shaxsning ijtimoiy kompetentligini shakllantiradi. Bular, shuningdek, ijtimoiy xavfsizlikni mustahkamlashga yordam beradi. Shaxsning bu qobiliyatlari ijtimoiy muhitda samarali muloqot qilish, xatoliklardan o'rganish va turli xil ijtimoiy rollarda muvaffaqiyatli faoliyat ko'rsatish uchun zarurdir.

Ijtimoiy stress va moslashuv: Ijtimoiy kompetentlikni rivojlantirishda stressni boshqarish muhim ahamiyatga ega. Jamiyatda turli ijtimoiy talablar va bosimlar mavjud bo'lib, ularga moslashish shaxsning psixologik holatiga ta'sir qilishi mumkin. Shaxslarning stressga qarshi kurashish qobiliyati va ijtimoiy vaziyatlarda moslashuvchanlik shaxsning ijtimoiy kompetentligini yaxshilaydi va uning ijtimoiy xavfsizligini ta'minlaydi.

Kiberya xavfsizligi va uning psixologik asosi

Kiberya xavfsizligining psixologik xususiyatlari:

Shaxsiy ma’lumotlarning maxfiyligi: Shaxsning onlayn xavfsizligini ta’minlash psixologik jihatdan odamlarning o‘z ma’lumotlarini boshqalar bilan bo‘lishishga nisbatan ehtiyotkorlik bilan munosabatda bo‘lishini talab qiladi. Kiberya xavfsizligi haqida tushuncha nafaqat texnologik, balki psixologik jihatdan ham muhimdir. Odamlar o‘z ma’lumotlari xavfsizligini his qilmasalar, bu ularning onlayn muhitdagi ishtirokini cheklaydi, ishonchni kamaytiradi va psixologik stressni oshiradi.

Xavfni boshqarish va stressni kamaytirish: Kiberya xavfsizligi va shaxsiy himoyaning ta’minlanishi ijtimoiy xavfsizlikni oshiradi, bu esa shaxslarning onlayn muhitda stress va xavfni boshqarishga oid psixologik ko‘nikmalarini rivojlantiradi. Xavfsizlik choralarining mavjudligi shaxsda ongli ravishda xavfsizligini his qilishni kuchaytiradi, bu esa umumiy psixologik barqarorlikni ta’minlaydi.

Kiberhujumlarga nisbatan psixologik javoblar: Kiberhujumlar va identifikatsiya o‘g‘irliklari kabi xavf-xatarlar shaxsda psixologik stress va xavotirlarni keltirib chiqarishi mumkin. Bunday holatlar shaxsning xavfsizlikka bo‘lgan ehtiyojlarini yanada kuchaytiradi. Xavfsiz tizimlarning mavjudligi, shaxsning xavfsizlikni ta’minlash bo‘yicha qarorlar qabul qilishda psixologik ishonchni oshiradi.

Shaxsiy xavfsizlikni ta’minlashda psixologik yondashuvlar: Kiberya xavfsizligi muammolari bilan bog‘liq bo‘lgan psixologik yondashuvlar o‘z ichiga axborotlarni himoya qilish, identifikatsiya o‘g‘irliklariga qarshi turish va kiberhujumlar haqida xabardor bo‘lishni oladi. Bu yondashuvlar, shuningdek, shaxslar uchun xavfsiz onlayn muhitni yaratishga yordam beradi, bu esa psixologik xavfsizlikni oshiradi.

Ijtimoiy kompetentlik va kibir xavfsizligini birlashtirish

Ijtimoiy kompetentlik va kibir xavfsizligi o‘rtasidagi aloqalar:

Ijtimoiy kompetentlik va kiberya xavfsizligini birlashtirishning ahamiyati: Ijtimoiy kompetentlik va kibir xavfsizligi o‘rtasidagi muvofiqlik shaxsning umumiy psixologik salomatligini va xavfsizligini ta’minlaydi. Onlayn va oflayn muhitdagi muvaffaqiyatli ijtimoiy aloqalar, o‘zaro hurmat va axborot xavfsizligini ta’minlash orqali shaxsning ijtimoiy barqarorligi mustahkamlanadi. Shaxslar onlayn muloqotlarda o‘zini xavfsiz his qilgan holda, samarali muloqot qilish, o‘z fikrlarini bildirish va boshqalar bilan hamkorlik qilishda muvaffaqiyatga erishadilar.

Texnologiyalar va psixologik yondashuvlar: Zamonaviy texnologiyalarning rivojlanishi bilan ijtimoiy kompetentlik va kibir xavfsizligi o‘rtasidagi o‘zaro aloqalar kuchayadi. Psixologik yondashuvlar, masalan, internetda xavfsiz muloqot va ma’lumot almashish qobiliyatlarini rivojlantirish orqali ijtimoiy kompetentlik va xavfsizlikni ta’minlash mumkin. Shuningdek, texnologik vositalar orqali xavfsizlikni ta’minlash, psixologik xavfsizlikni oshirishga yordam beradi.

Xulosa. Zamonaviy jamiyatda ijtimoiy kompetentlik va kibir xavfsizligi bir-birini to‘ldiradigan muhim komponentlardir. Ijtimoiy kompetentlik shaxsning boshqalar bilan samarali muloqot qilish va jamiyatga moslashish qobiliyatini rivojlantiradi, bu esa o‘z-o‘ziga ishonch va psixologik barqarorlikni ta’minlaydi. Kiberya xavfsizligi esa shaxsning onlayn muhitdagi xavfsizligini ta’minlab,

malumotlarining himoya qilinishiga yordam beradi. Ijtimoiy kompetentlik va kibir xavfsizligini birlashtirish, shaxsni xavfsiz va ishonchli his qilishga undaydi. Ushbu ikki omilning psixologik jihatlari zamonaviy shaxsning muvaffaqiyatli ijtimoiy va texnologik integratsiyasini qo‘llab-quvvatlaydi. Ijtimoiy kompetentlik va kibir xavfsizligini rivojlantirish orqali shaxslar o'zlarining psixologik xavfsizligini ta’minlashlari mumkin.

Adabiyotlar ro‘yxati:

1. Goleman, D. (1995). *Emotional Intelligence: Why It Can Matter More Than IQ*. Bantam Books.
Bu kitob ijtimoiy kompetentlik, empatiya va hissiy intellektning rivojlanishiga ta'sir qiluvchi psixologik omillarni tushuntiradi.
2. Shafir, E., & LeBoeuf, R. A. (2002). *Rationality and Decision Making: Psychological Perspectives*. Princeton University Press.
Ijtimoiy xavfsizlik va stressni boshqarish qobiliyatlari bilan bog‘liq psixologik qarorlar qabul qilish jarayonlari haqida.
3. Bandura, A. (1986). *Social Foundations of Thought and Action: A Social Cognitive Theory*. Prentice-Hall.
Banduraning ishlarida ijtimoiy kompetentlik va shaxsiy identifikatsiya, shuningdek, ijtimoiy o‘zaro munosabatlar va xavfsizlikni ta’minlash psixologiyasi haqida ko‘plab nazariyalar mavjud.
4. Mayer, J. D., Salovey, P., & Caruso, D. R. (2004). *Emotional Intelligence: Theory, Findings, and Implications*. Psychological Inquiry.
Ijtimoiy va hissiy intellektning rivojlanishi va uning psixologik xavfsizlikka ta’siri haqida ilmiy tadqiqotlar.

KIBERJINOYATCHILIKKA QARSHI KURASH VA YONG‘IN XAVFSIZLIGI: ZAMONAVIY TAHDIDLARGA QARSHI INTEGRATSIYALASHGAN YECHIMLAR

Xamrayev Rabbim Baxronovich

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti magistratura tinglovchisi

Kirish. Zamonaviy jamiyatda texnologiyalarning tez rivojlanishi bilan birga yangi xavflar ham yuzaga kelmoqda. Kiber jinoyatchilik va yong‘in xavfsizligi sohalari bugungi kunda alohida e’tibor talab qilayotgan sohalar bo‘lib, ular orasida o‘zaro bog‘lanish va birlashish zarurati kundan-kunga ortib bormoqda. Ushbu maqolada kiber jinoyatchilikka qarshi kurash va yong‘in xavfsizligini ta’minlashda yuzaga keladigan tahdidlar va bu sohalarda integratsiyalashgan yechimlar tahlil qilinadi.

Kiberjinoyatchilik: zamonaviy xavflar va tahdidlarga qarshi kurash

Kiber jinoyatchilik — bu axborot texnologiyalarini, internetni va boshqa raqamli resurslarni noqonuniy daromad olish yoki zarar yetkazish uchun ishlatishdir. Kiber jinoyatchilarning maqsadi ko‘pincha shaxsiy va korporativ ma’lumotlarni

o‘g‘irlash, tarmoqni buzish, yoki raqamli tizimlar orqali zarar yetkazishdir. So‘nggi yillarda kiber jinoyatchilarning faoliyati ko‘paygan va texnologiyalarning rivojlanishi bu jarayonni yanada murakkablashtirgan.

Kiber hujumlarning bir nechta asosiy turlari mavjud:

Fishinq: Foydalanuvchilarni aldagan holda ular haqida shaxsiy ma’lumotlarni yig‘ish.

Malware (zararli dasturlar): Kompyuter tizimlariga zarar yetkazuvchi yoki ma’lumotlarni o‘g‘irlaydigan dasturlar.

DDoS hujumlari: Maqsadli server yoki tarmoqni ishdan chiqarish uchun bir nechta kompyuterlardan bir vaqtda hujumlar amalga oshiriladi.

Bugungi kunda kiber jinoyatga qarshi kurashish uchun ilg‘or texnologiyalar, maxsus xavfsizlik tizimlari, va kiber-politsiya faoliyati talab qilinadi. Kiber xavfsizlik bo‘yicha kuchaytirilgan tartibga solish va innovatsion texnologiyalarni rivojlantirish, shu jumladan sun’iy intellekt yordamida kiber hujumlarni aniqlash, kiber jinoyatchilarni ushlashda samarali yechimlarni taqdim etadi.

Yong‘in xavfsizligi: jismoniy xavf va texnologiyalar

Yong‘in xavfsizligi — bu jismoniy muhitda yong‘inlarni oldini olish va ularga qarshi kurashishda foydalaniladigan barcha texnik va huquqiy tadbirlar yig‘indisidir. Yong‘in xavfsizligi tizimlari, asosan, binolar va infratuzilmalarda yong‘inlarning oldini olish, ularga tezkor javob berish, va jabrlanganlarni tezda evakuatsiya qilishga qaratilgan. Yong‘in xavfsizligini ta’minlash uchun yong‘in detektorlaridan, avtomatik yong‘in o‘chirish tizimlaridan va o‘zgartirilgan binolarni yong‘inlarga qarshi qayta loyihalash kabi texnologiyalar mavjud.

Yong‘in xavfsizligi tizimlarining samarali ishlashi uchun:

- **Yong‘in signallarini aniqlash tizimlari**.
- **Avtomatik yong‘in o‘chirish tizimlari** (masalan, sprinkel tizimlari).
- **Evakuatsiya marshrutlarini optimallashtirish**.

Yong‘in xavfsizligini ta’minlashda kiber xavfsizlik ham katta rol o‘ynaydi, chunki ko‘plab yong‘in xavfsizligi tizimlari raqamli infratuzilmalar bilan boshqariladi. Kiber hujumlar yong‘in xavfsizligi tizimlarining ishdan chiqishiga olib kelishi mumkin, bu esa jismoniy xavfni oshiradi.

Kiberjinoyatchilik va yong‘in xavfsizligi: integratsiyalashgan yechimlar

Bugungi kunda kiber jinoyatchilik va yong‘in xavfsizligi o‘rtasidagi bog‘lanish tobora kuchaymoqda. Yong‘in xavfsizligi tizimlarining raqamli boshqaruvi va kiber jinoyatchilikka qarshi kurashning integratsiyasi xavfsizlikni ta’minlashda muhim ahamiyatga ega. Kiber jinoyatchilar, masalan, yong‘in signalizatsiya tizimlarini buzish, yoki yong‘in o‘chirish tizimlarini ishdan chiqarish orqali xavfsizlikni zaiflashtirishi mumkin. Shu sababli, bu ikki soha o‘rtasida samarali integratsiya qilish zarur.

Quyidagi integratsiyalashgan yechimlar kiber jinoyatchilikka qarshi kurash va yong‘in xavfsizligini ta’minlashda muhim rol o‘ynaydi:

Kiber xavfsizlik va yong‘in xavfsizligi tizimlarini birlashtirish: Raqamli va jismoniy xavfsizlikni birlashtirgan tizimlar yaratish, bu tizimlar bir-birini to‘ldirib, xavfsizlikni yanada mustahkamlashga yordam beradi. Misol uchun, yong‘in xavfsizligi

tizimlarining raqamli tarmoqlarini himoya qilish, ular ustidan amalga oshirilgan kiber hujumlarga qarshi tarmoq xavfsizligini ta’minlash zarur.

Sun’iy intellekt va analitik tizimlarni qo‘llash: Sun’iy intellekt va mashina o‘rganish yordamida kiber hujumlarni oldindan aniqlash va yong‘in xavfsizligi tizimlaridagi noxush holatlarni tahlil qilish mumkin. Bunday tizimlar yordamida avtomatik ravishda xavflarni aniqlash va tezkor javob berish imkoniyatlari yaratiladi.

Xavfsizlikni nazorat qilish va ogohlantirish tizimlarini ishlab chiqish: Kiber xavfsizlik tizimlarining zaif joylarini aniqlash va yong‘in xavfsizligi tizimlarini kuzatib borish uchun yagona boshqaruv markazlari yaratish. Bunday tizimlar barcha xavfsizlik choralarini birlashtirib, xavflarga tezkor javob berishga imkon beradi.

Xalqaro hamkorlik va qonuniy normativlar: Kiber jinoyatchilik va yong‘in xavfsizligi bo‘yicha xalqaro hamkorlikni kuchaytirish, maxsus qonuniy tartiblar ishlab chiqish va xavfsizlik standartlarini ishlab chiqish. Bunday yondashuv global miqyosda xavfsizlikni ta’minlashga yordam beradi.

Xulosa. Kiber jinoyatchilik va yong‘in xavfsizligi bugungi kunda alohida e’tibor talab qiluvchi sohalar bo‘lib, ularning o‘zaro bog‘lanishi va integratsiyalashuvi jamiyatni yanada xavfsizroq qilish uchun zarurdir. Kiber hujumlar va jismoniy xavfli vaziyatlar o‘rtasidagi bog‘lanishni tushunish va bu sohalarda samarali yechimlarni ishlab chiqish jamiyat uchun yuqori darajadagi xavfsizlikni ta’minlashga yordam beradi. Kiber xavfsizlik va yong‘in xavfsizligini birlashtirish, ilg‘or texnologiyalar va xalqaro hamkorlik orqali zamonaviy tahdidlarga qarshi samarali kurashish mumkin.

Adabiyotlar:

1. **Kshetri, N.** (2017). *Cybercrime and Cybersecurity in the Global South*. Springer.
2. **Pfleeger, S. L., & Pfleeger, C. P.** (2015). *Security in Computing*. Prentice Hall.
3. **Erl, T.** (2016). *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*. Prentice Hall.
4. **Fire Protection Research Foundation** (2020). *Fire Safety and Security: The Role of Technology in Modern Fire Prevention*. Fire Protection Research Foundation.

KIBERJINOYATCHILIKKA QARSHI KURASHISH JARAYONIDAGI MUAMMOLAR VA SUN’IY INTELLEKTDAN FOYDALANISHNING AFZALLIKLARI

Abdulloyev Daler Amrilloyevich

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti magistratura tinglovchisi

Kirish. Bugungi kunda kiberjinoyatchilik butun dunyo miqyosida jiddiy tahdidga aylangan. Internetning keng tarqalishi va raqamli texnologiyalarning rivojlanishi kiberjinoyatlar sonining ortishiga olib keldi. Kiberjinoyatchilik, masalan, shaxsiy ma’lumotlarni o‘g‘irlash, kompyuter tizimlariga noqonuniy kirish, firibgarlik va tarmoq hujumlari kabi turli shakllarda yuzaga kelishi mumkin. Shu sababli, kiberjinoyatchilikka qarshi kurashish jiddiy ahamiyat kasb etadi. Ushbu maqolada

kiberjinoyatchilikka qarshi kurashish jarayonidagi asosiy muammolar va sun’iy intellekt (SI) texnologiyalaridan foydalanishning afzalliklari haqida so‘z boradi.

Kiberjinoyatchilikka qarshi kurashishdagi muammolar

Yangi va murakkab usullar Kiberjinoyatchilik tez rivojlanayotgan soha bo‘lib, jinoyatchilar doimo yangi usullarni ishlab chiqib, xavfsizlik tizimlarini aldashga harakat qilmoqda. Kiberxurujlar, phishing, trojan viruslari va botnet tarmoqlari kabi turli xil hujum usullari mavjud. Bu jinoyatchilarni aniqlash va ushlash jarayonini juda murakkablashtiradi.

Global xususiyat Kiberjinoyatchilik global muammo hisoblanadi, chunki internet orqali jinoyatlar mamlakatlar o‘rtasida cheksiz tarzda tarqalishi mumkin. Bu esa milliy va xalqaro huquqni buzish, sud ishlarini va jinoyatchilarni jazolashni qiyinlashtiradi. Kiberjinoyatlar ko‘pincha chegaralarni bilmaydi, bu esa xalqaro hamkorlikni ta’minlashda to‘siqlar yaratadi.

Resurslar va mutaxassislar etishmasligi Kiberjinoyatchilikka qarshi kurashishda davlatlar va xususiy sektorlar ko‘pincha yetarli resurslar va malakali mutaxassislarga ega emas. Texnologiyalar juda tez o‘zgarib borayotganligi sababli, mutaxassislarning doimiy ravishda yangilanib turishi zarur, bu esa qo‘shimcha resurslar talab qiladi.

Maxfiylik va huquqlarni himoya qilish Kiberjinoyatchilikka qarshi kurashishda ko‘pincha fuqarolarning shaxsiy hayoti va ma’lumotlarini himoya qilish bilan bog‘liq muammolar yuzaga keladi. Xavfsizlikni ta’minlash uchun tizimlarga kirish va ma’lumotlarni tekshirish kerak bo‘lsa-da, bu holat maxfiylik va huquqlarni buzmaslik nuqtai nazaridan murakkabliklar yaratadi.

Sun’iy intellektning kiberjinoyatchilikka qarshi kurashishdagi afzalliklari

Hujumlarni aniqlash va oldini olish Sun’iy intellekt algoritmlari xavfsizlik tizimlarida foydalanuvchi xatti-harakatlarini tahlil qilish va anomal faoliyatni aniqlashda samarali ishlaydi. Masalan, kompyuter tizimlarida o‘zgarishlarni kuzatib boruvchi SI algoritmlari kiberxurujlarni vaqtida aniqlab, oldini olish imkoniyatini beradi. Ular foydalanuvchi xatti-harakatlarini o‘rganib, shubhali va noma’lum faoliyatlarni avtomatik tarzda tahlil qilishi mumkin.

Avtomatlashtirilgan tahlil va ma’lumotlarni qayta ishlash Sun’iy intellekt yordamida katta hajmdagi ma’lumotlar tez va samarali tarzda tahlil qilinadi. Kiberjinoyatchilar tomonidan amalga oshirilgan xatti-harakatlar odatda ma’lumotlar bazalarida kuzatiladi. SI tizimlari bu ma’lumotlarni avtomatik ravishda qayta ishlab, jinoyatlarni aniqlash jarayonini tezlashtiradi. Bu esa tahlil qilishda inson faktori tufayli yuzaga keladigan xatoliklarni kamaytiradi.

Tarmoqni kuzatish va monitoring qilish. Sun’iy intellekt yordamida tarmoqdagi barcha faoliyatlar, jumladan, xakerlik hujumlarini aniqlash va ularni bartaraf etish osonlashadi. SI tizimlari tarmoqdagi noxush harakatlarni tezda aniqlab, avtomatik ravishda himoya choralarini ko‘rish imkoniyatini yaratadi. Bunday tizimlar tarmoqni 24/7 monitoring qilib, har qanday xavf-xatarni aniqlashda eng yaxshi yordamchi bo‘ladi.

Kiberjinoyatchilarni izlash va ushlashda yordam. Sun’iy intellekt kiberjinoyatchilarni izlashda va ularni ushlashda yordam beradigan qator vositalar yaratishga imkon beradi. SI tizimlari jinoyatchilarning onlayn faoliyatini tahlil qilib, ularning identifikatsiyasini osonlashtiradi. Shuningdek, bu texnologiyalar

kiberjinoyatlarni tekshirish va jinoyatlarni hal qilish jarayonida vaqtni qisqartirishga yordam beradi.

Xulosa. Kiberjinoyatchilikka qarshi kurashish dunyodagi barcha davlatlar uchun jiddiy muammo hisoblanadi. Yangi texnologiyalar va jinoyatchilarning murakkab usullari bu kurashni yanada qiyinlashtiradi. Shu bilan birga, sun'iy intellektning imkoniyatlaridan foydalanish, kiberjinoyatchilikka qarshi kurashishda sezilarli afzalliklar yaratadi. Hujumlarni aniqlash va oldini olish, avtomatlashtirilgan tahlil va ma'lumotlarni qayta ishlash, tarmoqni monitoring qilish va jinoyatchilarni izlash kabi afzalliklar SI texnologiyalarini kiberxavfsizlikda muhim vositaga aylantiradi. Shu sababli, davlatlar va kompaniyalar sun'iy intellektni o‘z xavfsizlik tizimlariga integratsiya qilishni davom ettirishlari zarur.

Adabiyotlar:

1. **Badaoui, M., & Khoukhi, L. (2021).** "Artificial Intelligence for Cybersecurity: Techniques, Applications, and Challenges." *Springer*.
Ushbu kitobda sun'iy intellekt texnologiyalarining kiberxavfsizlik sohasidagi qo‘llanilishi va bu sohada yuzaga keladigan muammolar haqida batafsil ma'lumot berilgan.
2. **Deloitte (2020).** "Cybercrime: An Evolving Threat." *Deloitte Insights.*
Deloitte-ning ushbu hisobotida kiberjinoyatchilikning rivojlanishi va global miqyosda sun'iy intellektdan qanday foydalanish mumkinligi to‘g‘risida muhokama qilinadi.
3. **Buczak, A. L., & Guven, E. (2016).** "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection." *IEEE Communications Surveys & Tutorials.*
Ushbu maqola kiberxavfsizlikka oid turli intruziya aniqlash usullarini, shu jumladan, sun'iy intellekt asosidagi yondashuvlarni tahlil qiladi.
4. **Kshetri, N. (2017).** "1 Cybercrime and Cybersecurity in the Age of Cloud Computing." *Springer International Publishing.*
Kitob kiberjinoyatchilik va kiberxavfsizlikni bulutli hisoblash texnologiyalarida qanday ta'sir qilishini va sun'iy intellektning bu jarayondagi rolini ko‘rib chiqadi.

KIBER JINOYATCHILIK VA UCHUVCHISIZ UCHISH APPARATI TEXNOLOGIYALARINING XAVFLI IJTIMOIY TA'SIRI: XAVFSIZLIK, NAZORAT VA KURASHISHDA YANGI MUAMMOLAR VA YECHIMLAR

Xotamov Qodirjon Axberdi o‘g‘li

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti magistratura tinglovchisi

Bugungi kunda texnologiyalarning tez rivojlanishi jamiyatga yangi imkoniyatlar yaratish bilan birga, bir qator xavf-xatarlarni ham keltirib chiqarmoqda. Kiber jinoyatchilik va uchuvchisiz uchish apparatlari (dronlar)ning birlashuvi, ayniqsa, xavfsizlik va jamiyatning barqarorligini tahdid qilishda muhim omil bo‘lib qolmoqda. Ushbu maqolada kiber jinoyatchilik va dronlar texnologiyalarining ijtimoiy ta'siri, bu tahdidlarga qarshi kurashishdagi yangi muammolar va mumkin bo‘lgan yechimlar ko‘rib chiqiladi.

Kiberjinoyatchilik: yangi tahdidlar va xavfli ko‘rinishlar

Kiber jinoyat — bu axborot texnologiyalarini va internetni noqonuniy daromad olish, shaxsiy ma’lumotlarni o‘g‘irlash, tarmoqlarni buzish, yoki axborot tizimlariga zarar yetkazish uchun ishlatishdir. So‘nggi yillarda kiber jinoyatchilikning ko‘lami ancha kengaygan va texnologiyalarning rivojlanishi bu jarayonni yanada murakkablashtirgan. Kiber jinoyatga kiruvchi turli harakatlar orasida, masalan, tarmoqni buzish, shaxsiy ma’lumotlarni o‘g‘irlash, soxta identifikatsiya yaratish va raqamli hujumlar mavjud.

Dronlar texnologiyasi esa, o‘zining yuqori aniqlikdagi kuzatuv va manipulyatsiya imkoniyatlari bilan kiber jinoyatchilarga yangi imkoniyatlar yaratmoqda. Kiber jinoyatchilar, dronlarni foydalanib, maxfiy ma’lumotlarni o‘g‘irlash, noxush videolarni tarqatish yoki maxfiy hududlarni ko‘rib chiqish uchun ishlatishlari mumkin.

Uchuvchisiz uchish apparati (dronlar): texnologik salohiyat va ta’sir

Uchuvchisiz uchish apparatlari (dronlar) hozirgi kunda nafaqat harbiy va ilmiy sohalarda, balki tijorat, xavfsizlik va qishloq xo‘jaligi kabi sohalarda ham keng qo‘llanilmoqda. Dronlar masofaviy boshqarilishi va yuqori aniqlikdagi tasvir olish imkoniyatlari tufayli juda foydali texnologiyalar sifatida qaraladi. Ular, shuningdek, ijtimoiy hayotga ta’sir ko‘rsatishi mumkin.

Ammo, dronlarning texnologik imkoniyatlari ularga zararli maqsadlar uchun ham ishlatilishiga imkon beradi. Masalan, dronlar orqali kiber hujumlar amalga oshirilishi, maxfiy tasvirlar olish yoki hatto zararli materiallar tarqatish mumkin. Bunday texnologiyalar jamiyatni xavf ostiga qo‘yadi.

Kiberjinoyat va dronlarning birlashuvi: yangi xavf-xatarlar

Kiber jinoyatchilar va dronlar texnologiyalarining birlashuvi xavfli yangi tahdidlarni keltirib chiqaradi. Quyidagi xavflarni ko‘rib chiqish mumkin:

Maxfiy axborotlarning o‘g‘irlanishi: Dronlar yordamida maxfiy ma’lumotlar yoki shaxsiy ma’lumotlar o‘g‘irlanishi mumkin. Dronlar odamlarni kuzatish, noxush ma’lumotlarni yig‘ish yoki maxfiy hududlarga kirish imkoniyatiga ega.

Tarmoqni buzish va manipulyatsiya qilish: Kiber jinoyatchilar dronlar yordamida axborot tarmoqlarini buzish yoki maxfiy axborot tizimlariga kirish orqali zarar yetkazishlari mumkin. Ular, masalan, dronlar orqali serverlar va ma’lumot markazlariga tajovuz qilishlari mumkin.

Jismoniy xavf yaratish: Dronlar yordamida portlovchi moddalar yoki zararli materiallar yuborish, odamlarni kuzatish yoki muhim infrastrukturalarga hujum qilish mumkin. Bu holat nafaqat axborot xavfsizligini, balki jismoniy xavfsizlikni ham tahdid qiladi.

Tashkiliy tartibni buzish: Kiber jinoyatchilar dronlar yordamida davlat yoki korporativ tizimlarni manipulyatsiya qilishlari mumkin. Bu, o‘z navbatida, iqtisodiy, siyosiy va ijtimoiy barqarorlikka jiddiy ta’sir ko‘rsatishi mumkin.

Kiberjinoyat va dronlarga qarshi kurashish: yechimlar va nazorat

Kiber jinoyat va dronlar texnologiyalarining salbiy ta’siridan himoya qilish uchun quyidagi yechimlar ko‘rib chiqilishi zarur:

Texnologik nazorat va xavfsizlikni kuchaytirish: Dronlar va kiber xavfsizlik texnologiyalarini rivojlantirish kerak. Dronlar orqali kiber hujumlarni aniqlash va ularga qarshi kurashishda ilg‘or algoritmlar va maxsus texnologiyalar ishlab chiqilishi zarur. Shuningdek, dronlar yordamida zararli materiallarni tarqatish holatlariga qarshi himoya mexanizmlarini yaratish lozim.

Yangi qonunlar va huquqiy me’yorlar ishlab chiqish: Kiber jinoyat va dronlar bilan bog‘liq huquqiy normalarni takomillashtirish muhimdir. Bu huquqiy nazorat joriy etish va dronlarning xavfsiz foydalanishini ta’minlashga yordam beradi. Dronlar ishlab chiqaruvchilari va foydalanuvchilari uchun ma’lum standartlar va cheklovlar belgilanadi.

Kengaytirilgan xabardorlik va ta’lim: Jamiyat va mutaxassislar o‘rtasida kiber xavfsizlik va dronlar bilan ishlashga doir xabardorlikni oshirish muhimdir. Odamlarni dronlardan va kiber hujumlardan qanday himoyalanish haqida ta’lim berish kerak.

Global hamkorlikni kuchaytirish: Kiber jinoyatchilik va dronlar bilan kurashishda xalqaro hamkorlikni kuchaytirish zarur. Kiber xavfsizlikka qarshi kurashishda xalqaro normativlar va standartlar o‘rnatilishi kerak.

Xulosa. Kiber jinoyatchilik va uchuvchisiz uchish apparatlari texnologiyalarining birlashuvi jamiyat uchun yangi xavf-xatarlar yaratmoqda. Bu tahdidlarga qarshi kurashish uchun ilg‘or texnologiyalar, huquqiy tartib va xalqaro hamkorlik zarur. Texnologik taraqqiyot o‘zgaruvchan tahdidlarga olib kelishi mumkin, ammo to‘g‘ri choralar ko‘rilganda, bu xavflarni minimallashtirish va xavfsizlikni ta’minlash mumkin. Shuningdek, jamiyatni bunday tahdidlarga qarshi tayyorlash va har tomonlama himoya qilish uchun yangi mexanizmlar ishlab chiqish zarur.

Adabiyotlar:

1. **Bary, M., & McAfee, A.** (2019). *Cybersecurity: The Essential Guide to Protecting Your Organization’s Digital Assets*. Wiley.
2. **Shin, D. H., & Hwang, H.** (2020). *Drone Technology: A Review of Uses, Applications, and Challenges in Cybersecurity*. Springer.
3. **Sundararajan, V.** (2018). *The Digital Economy: Rethinking the Role of Technology in the Future of Work*. MIT Press.
4. **Kshetri, N.** (2017). *Cybercrime and Cybersecurity in the Global South*. Springer.

KIBERXAVFSIZLIK SOHASIDAGI JINOYATLARINING OLDINI OLISH MASALARI

Habibullayev Sayfiddin Saydullo o‘g‘li, Musayev Hamzahon Zokirjon o‘g‘li

Namangan davlat unversiteti Yurdik fakulteti 2-bosqich talabalari

Annontatsiya. Ushbu maqolada, kiberxavfsizlik va kiberhuquq tushunchalari va ayni vaqtda O‘zbekistonda kiberjinoyatlar, hozirgi kundagi kiberxavfsizlik muammolar va kiberjinoyatlarga qarshi kurashish, kiber jinoyatchilikning turlari, kiberjinoyatchilikning oldini olish usullari, ular aholining qaysi qatlami orasida ko'proq sodir bo'layotgani, ulardan qanday himoyalanish zarurligi, kiber jinoyatchilikka qarshi aholining barcha qatlami orasida huquqiy ong va madaniyatni

rivojlantirish va fuqarolar kiberjinoyatlardan qanday himoya qilish mumkinligi haqida ma’lumotlarni yetkazish masalalr ko‘rib chiqiladi.

Kalit so‘zlar: Kiberxavfsizlik, CSEC2017 Joint Task Force ,meynfreym kompyuterlar, Cisco tashkiloti, Kiber huquq, Axborot xavfsizligi, CCTV (josuslik qilish va aloqalarni kuzatish uchun veb-kameralar), cryptojacking, kiber-josuslik,kiber-shantaj.

Kiberxavfsizlik bizning davrimizda, ayniqsa sodir bo‘layotgan barcha texnologik yutuqlar bilan chambarchas bog‘langan. Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo‘lib, unga berilgan turlicha ta’riflar mavjud. Xususan, CSEC2017 Joint Task Force manbasida kiberxavfsizlikka quyidagicha ta’rif berilgan:

Kiberxavfsizlik – hisoblashlarga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni to‘g‘ri bajarilishini kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonlarni mujassamlashtiradi. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o‘z ichiga oladi. Kiberxavfsizlik ta’limning mujassamlashgan bilim sohasi bo‘lib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o‘z ichiga oladi.

Kiberxavfsizlik sohasining zaruriyati birinchi meynfreym kompyuterlar ishlab chiqarilganidan boshlab paydo bo‘la boshlagan. Bunda mazkur qurilmalarning va ularning vazifalarining himoyasi uchun ko‘p sathli xavfsizlik choralari amalga oshirilgan. Milliy xavfsizlikni ta’minlash zaruriyatini oshib borishi kompleks va texnologik murakkab ishonchli xavfsizlik choralarini paydo bo‘lishiga sabab bo‘ladi. Hozirda axborot texnologiyalari sohasida faoliyat yuritayotgan har bir mutaxassisning kiberxavfsizlikning fundamental bilimlariga ega bo‘lishi talab etiladi.

Shuningdek, hozirgi kunda odamlar orasida keng tarqalayotgan jinoyatlardan biri bu kiberjinoyatidir.

Kiberjinoyat bu — kompyuter va tarmoqlarning birgalikdagi aloqasi ostida sodir etiluvchi jinoyat turi. Kompyuter jinoyat paytida maqsadli yo‘naltirilgan qurol vazifasini bajarib beradi. Kiberjinoyat kimningdir xavfsizligi va moliyaviy saviyasiga zarar yetkazish maqsadida sodir etiladi.

Maxfiy ma’lumotlar qonuniy tarzda himoyalangan holatda yuz beruvchi kiberjinoyatlar bilan bog‘liq ko‘pgina jinoyatlar mavjud. Xalqaro miqyosda hukumat ham, nodavlat subyektlar ham kiberjinoyatlar, jumladan, josuslik, moliyaviy o‘g‘irlik va boshqa transchegaraviy jinoyatlar bilan shug‘ullanadi. Xalqaro chegaralarni kesib o‘tuvchi va kamida bitta milliy davlatning xatti-harakatlarini o‘z ichiga olgan kiberjinoyatlar ba’zan kiberurush deb ataladi. Uorren Baffet kiberjinoyatni „insoniyatning birinchi raqamli muammosi“deb ta’riflaydi va „insoniyat uchun real xavf tug‘diradi“, deya qo‘shimcha qilib o‘tadi[70].

Kiberjinoyatni butunlay yo‘q qilish va to‘liq internet xavfsizligini ta’minlash imkoni bo‘lmasa-da, korxonalar tizimlar, tarmoqlar va ma’lumotlar xavfsizligini ta’minlashga chuqur mudofaa yondashuvidan foydalangan holda samarali kiberxavfsizlik strategiyasini qo‘llab-quvvatlash orqali uning ta’sirini kamaytirishga erishish mumkin. Kiber jinoyatlarni kamaytirish yo‘llari;

[70] https://uz.wikipedia.org/wiki/Bosh_Sahifa

-biznes va xodimlar uchun aniq siyosat va tartiblarni ishlab chiqish;

-ushbu siyosat va protseduralarni qo‘llab-quvvatlash uchun kiberxavfsizlik hodisalariga javob rejalarini yaratish;

- tizimlar va korporativ ma’lumotlarni himoya qilish bo‘yicha amaldagi xavfsizlik choralarini belgilash;

-ikki faktorli autentifikatsiya (2FA) ilovalari yoki jismoniy xavfsizlik kalitlaridan foydalanish;

- imkoni bo‘lganda, har bir onlayn hisobda 2FA ni faollashtiring;

-moliyaviy menejer bilan gaplashish orqali pul jo‘natish bo‘yicha so‘rovlarning haqiqiyligini og‘zaki tekshirish;

- kompaniya elektron pochta xabarlariga o‘xshash kengaytmali elektron pochta xabarlarini belgilovchi tajovuzlarni aniqlash tizimi (IDS) qoidalarini yaratish;

- so‘rovlar odatiy emasligini aniqlash uchun pul mablag‘larini o‘tkazish bo‘yicha barcha elektron pochta so‘rovlarini diqqat bilan ko‘rib chiqish;

-xodimlarni kiberxavfsizlik siyosati va tartib-qoidalari hamda xavfsizlik buzilgan taqdirda nima qilish kerakligi bo‘yicha doimiy ravishda o‘qitish;

-veb-saytlar, so‘nggi nuqta qurilmalari va tizimlarini barcha dasturiy ta’minot yangilanishlari yoki yamoqlari bilan joriy qilish;

- ransomware hujumi yoki ma’lumotlar buzilgan taqdirda zararni kamaytirish uchun ma’lumotlar va ma’lumotlarni muntazam ravishda zaxiralash.

Kibermakondagi muammolardan biri bu yurisdiktsiyani aniqlashdir. Internet global bo‘lganligi sababli, muayyan vaziyatga qaysi qonunlar qo‘llanilishini aniqlash qiyin bo‘lishi mumkin. Kiberhuquq kibermakondagi yurisdiktsiya masalalarini hal qiluvchi qoidalar va qoidalarni o‘z ichiga oladi, Fuqarolik va tijorat masalalari bo‘yicha sud qarorlarini ijro etish va sud qarorlarini ijro etish to‘g‘risidagi Gaaga konventsiyasi.

Kiberhuquq faqat ayrim mamlakatlar bilan chegaralanib qolmaydi. Internet global bo‘lgani uchun kibermakonni tartibga solishda xalqaro huquq ham rol o‘ynaydi. Kiber huquq xalqaro bitimlar va munosabatlarni tartibga soluvchi qoidalar va qoidalarni o‘z ichiga oladi, masalan, Birlashgan Millatlar Tashkilotining Xalqaro shartnomalarda elektron aloqalardan foydalanish to‘g‘risidagi konventsiyasi.

Kiberhuquq jismoniy shaxslar uchun ham muhim ahamiyatga ega. Shaxslar internet va tegishli texnologiyalardan foydalanishda o‘z huquq va majburiyatlarini bilishlari kerak. Kiber qonunlarga rioya qilmaslik shaxslar uchun huquqiy va moliyaviy oqibatlarga olib kelishi mumkin, masalan, shaxsiy ma’lumotlarni o‘g‘irlash va kiber ta'qib qilish, ammo kiber qonunlarni tushunish va ularga rioya qilish shaxslarga shaxsiy ma’lumotlarini himoya qilish va maxfiyligini ta’minlashga yordam beradi.

Shuningdek, biz raqamli dunyoda yashayapmiz, hayotimizni internetsiz, virtual olamsiz tasavuur eta olmaymiz. Ma’lumotni saqlash yoki ma’lumotlarga kirish bo‘ladimi, biz bunday ishlarni bajarish uchun internetdan yordam so‘raymiz. Virtual olamni dunyoga tobora ortib borayotgan aralashishi bizni kiber tahdidlarga moyil qilmoqda. Hech shubha yo‘qki, kiber jinoyatlar eksponensial sur'atda o‘sib bormoqda.

Internetda foydalangan holda jinoyatchilar yoki xakerlar internet foydalanuvchilarining shaxsiy ma’lumotlariga kirib, ulardan o‘z manfaati uchun foydalanmoqda, tovlamachilik, firibgarlik kabi jinoyatlarni virtual olamda sodir

etishmoqda[71]. Statistik ma’lumotlarga ko‘ra, o‘tgan davr mobaynida global sanoatning 85 foizi fishing va ijtimoiy muhandislik kiberhujumlarini boshdan kechirdi[72].

Innovatsion texnologiyalar va kibermexanizmlarning kiritilishi bilan internet jinoyatchilari har qachongidan ham kuchliroq bo‘lib bormoqda. Ular doimiy ravishda internet olamiga hujum qilib, maxfiy ma’lumotlarni buzmoqda. Kiberjinoyatchilar doimo oson yondashuvlar orqali katta pul ishlash yo‘llarini izlaydilar. Ularning asosiy maqsadlari cheksiz miqdordagi maxfiy ma’lumotlarga ega bo‘lgan transmilliy kompaniyalar va boy biznesmenlardir. Agar biz o‘ylab ko‘rsak, bizni internetga yaqinlashtiradigan har qanday narsa bizni kiberhujumlarga duchor qilishi mukin.

O‘tkazilgan tahlil natijalari bugungi kunda mamlakatda kiberjinoyatchilikning o‘sish tendensiyasi kuzatilayotganidan dalolat bermoqda.

So‘nggi 3 yilda kiberjinoyatlar soni bir necha baravarga oshib ketgan. Jumladan, kiberjinoyatchilikning bir qator turlari sodir bo‘layotgani kuzatilmoqda. Ular quyidagicha:

1. firibgarlar plastik karta foydalanuvchilariga kelgan SMS-xabarnomadagi kodlarni to‘lovni amalga oshirish, yutuqni berish kabi bahonalar orqali egallab, undagi mablag‘larni o‘zlashtirishi;

2. shaxsiy ma’lumotlarni egallash va ularni oshkor qilish bilan qo‘rqitib tovlamachilik qilishi (kibertovlamachilik);

3. ijtimoiy tarmoqda zo‘rlik ishlatish bilan qo‘rqitishi, haqorat, suitsid holatlari (kiberbulling) va boshqalar hozirda yurtimizdagi kiberjinoyatlarning oshib borayotgan turlari hisoblanadi[73]. Ushbu holatlar milliy qonunchilikni takomillashtirish, davlat tomonidan huquqiy tizimda xalqaro huquqiy normalar ustuvorligini tan olish prinsipi asosida tegishli xalqaro huquqiy normalarga milliy huquq tizimini moslashtirish, ularning mazmunini singdirish hamda kiberjinoyatchilikni oldini olishga qaratilgan xalqaro konvensiya, shartnomalarga qo‘shilishni taqozo etmoqda.

Kiberjinoyatlarning keng tarqalishi va xorijiy, ko‘p, o‘zgaruvchan yoki noma’lum yurisdiksiyalarda joylashgan bo‘lishi mumkin bo‘lgan elektron dalillarni olishning murakkablashishi bilan huquqni muhofaza qilish organlarining vakolatlari hududiy chegaralar bilan cheklanadi. Natijada, davlatlarning vakolatli organlariga ma’lum bo‘lgan kiberjinoyatlarning faqat kichik bir qismi bilan kurashish mumkin bo‘lib qoladi.

Bunga qarshi turish uchun xalqaro shartnomalarga qo‘shilish, hukumatlararo o‘zaro yordamning yo‘lga qo‘yilishi kiberjinoyatlarga qarshi samarali kurashishda muhim ro‘l o‘ynaydi.

Xulosa qilib aytadigan bo‘lsak,kiberxavfsizlikni ta’minlash va kiberjinoyatlarning oldini olish uchun qttor davlatlar va tashkilotlar o‘z qonun hujjatlarini qabul qilgan va O‘zbekistonda ham birin ketin kiberjinoyatchillikga oid masalalar birin ketin ko‘rib chiqilmoqda.Kiberxavfsizliknin yaxshilash va kiberjinoyatlarning oldini olish uchun quydagi takliflar berish samarali deb hisoblayman.

[71] . https://www.jigsawacademy.com/blogs/cyber-security/major-causes-of-cyber-crimesyou-must-be-aware-of/
[72] https://earthweb.com/cybercrime-statistics/
[73] . https://zamon.uz/detail/ozbekistonda-songgi-3-yilda-kiberjinoyatlar-keskin-oshganozbekiston

Birinchidan, Mamlakatimizda mavjud bo‘lgan qonunchilikdagi bo`shliqlarni aniqlash va yangilash. Ya’niy Kiberxavfsizlik bo`yicha qonunchilikni takomillashtirishning birinchi bosqichi bo`shliq va kamchiliklarni aniqlash uchun amaldagi qonun va me`yoriy hujjatlarni qayta ko`rib chiqishdan iborat. Barcha kiberxavfsizlikga oid normativ huquqiy hujjatlarni aniqlab yangilash faol natija ko‘rsata oldi. Bundan tashqari,yangi qonunlar qabul qilish bilan birga aholini ogohlikka chaqirish orqali kiberxafvsizlikni oshirish.Kiberxavfsizlik nafaqat hukumatning, balki shaxslar va tashkilotlarning ham amalga oshirishi kerak bo`lgan vazifalaridan biri hisoblanadi. Shu bois keng jamoatchilik, korxonalar va davlat amaldorlari o`rtasida kiberxavfsizlik bo`yicha xabardorlikni oshirish va ta`limni kuchaytirish zarur.

Ikkinchidan turli xil agentliklar kabi Kiberxavfsizlik agentligini tashkil etish zarur. Milliy kiberxavfsizlik strategiyasini muvofiqlashtirish va amalga oshirish uchun kiberxavfsizlik uchun mas'ul bo‘lgan markazlashtirilgan agentlik tashkil etilishi kerak. Ushbu agentlik kibertahdidlarni samarali hal qilish uchun yetarli darajada xodimlar va resurslar bilan ta'minlanishi kerak. Shuningdek ular uchun alohida e’tibor beish kerak va ularning ishini keyinchalikn yaxshilash uchun qonun ham qabul qilish maqsadga muvafiq bo‘ladi.

Uchunchidan, davlat barcha organlari o‘rtasida aniq va qonuniy ma’lumotlarni almashishini ta’minlash kerak.Bu bilan davlat kiberjinoyatlarning oldini olish usullarini ko‘rishi mumkin. Misol tariqasida aytadigan bo‘lsak Davlat xavfsizlik xizmati barcha ma’lumotlar bazasi HMQO lar bilan almashishishi yoki HMQO ma’lumotlar bazasini DXX tekshirishg kerakligi bunda bir biri bilan ma’lumotlar almashish jarayonida ularda mavjud bo‘lgan kiberxavfsizlikga oid muomolari bilishadi va kiberjinoyatlar kelib chiqishining oldini olishi mumikin.

FOYDALANILGAN ADABIYOTLAR

1.O‘zbekiston Respublikasi Konstitutsiyasi 2023 lex.uz

2. “Axborot texnologiyalari va kommunikatsiyalari to‘g‘risida”gi qonun https://lex.uz/docs/-3564970

3. "Tezkor-qidiruv faoliyati to‘g‘risida"gi qonun https://lex.uz/ru/docs/-2107763?ONDATE=21.04.2021%2000

4. “Davlat siri to‘g‘risida”gi qonun https://lex.uz/ru/docs/-98850

5. Kiber huquq – huquq sohasi sifatida: risola / tuzuvchilar R.R.Shakurov, M.M.Vohidov. – Toshkent: O‘zbekiston Respublikasi Adliya vazirligi qoshidagi Yuristlar malakasini oshirish markazi, 2022. – 27 b

6. https://uz.wikipedia.org/wiki/Bosh_Sahifa

7. CENTRAL ASIAN JOURNAL OF EDUCATION AND INNOVATION SJIF www.in-academy.uz

8.https://www.jigsawacademy.com/blogs/cyber-security/major-causes-of-cyber-crimesyou-must-be-aware-of/

9.https://earthweb.com/cybercrime-statistics/

10.https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime

YANGILANOYOTGAN O‘ZBEKISTONDA KIBERJINOYATLARNI OLDINI OLISH USULLARI

Normurodov Elbek Bunyod o‘g‘li, Shukurulloev Shodiyor To‘rajonzola

Namangan davlat universiteti Yuridik fakulteti talabalari

Annotatsiya. Mazkur maqolada rivojlanayotgan O‘zbekistondagi kiberjinoyatlarni oldini olish usullari, ya’ni yaqin kelajakda bo‘lishi mumkin bo‘lgan va o‘tmishda bo‘lgan bir qator kiberjinoyatlarni takrorlanishini oldini olish masalalari bo‘yicha bir qator fikr va mulohazalar bayon etilgan.

Kalit so‘zlar: kiberjinoyat, kiberxavfsizlik, xakker, “Lazarus”, “Kaspersky”, firibgarlik, bank-moliya operatsiyalari, link

XXI asr - axborot texnologiyalari asri deya atalayotgan bir vaqtda har bir shaxsdan texnologiyalarni o'rganish, ular haqida bilimga ega bo'lish zamon talabi darsjasiga chiqdi. Rivojlangan texnologiyalar, mobil telefonlar, kompyuterlar va turli xil gadjetlar hayotimizda turli xil qulay imkoniyatlarni yaratdi, masalan, siz kompyuter yoki telefonlar orqali uydan chiqmasdan turib xarid qilishingiz, buyurtma berishingiz, hattoki daromad qilishingiz ham mumkin. Lekin ushbu yaratilgan imkoniyatlardan noto'g'ri maqsadlarda, ya'ni kiberjinoyatlarni amalga oshirishda foydalanayotgan shaxslar ham jamiyatimizda paydo bo'lmoqda. Ushbu kiberjinoyatlarni oldini olish maqsadida turli xil usul va uslublar ishlab chiqilmoqda.

Kiberjinoyatlar (inglizcha: cybercrime) – bu axborot texnologiyalari, kompyuter tarmoqlari yoki internetdan foydalangan holda sodir etiladigan noqonuniy harakatlar bo‘lib, ularga firibgarlik, shaxsiy ma’lumotlarni o‘g‘irlash, kompyuter tizimlarini buzish, noqonuniy dasturlar yaratish va tarqatish, moliyaviy ma’lumotlarga ruxsatsiz kirish kabi jinoyatlar kiradi.

Kiberjinoyatlar ikki asosiy turga bo‘linadi, kompyuter vositasida sodir etiladigan jinoyatlar – bu holda kompyuter jinoyat quroli sifatida ishlatiladi, ya'ni jinoyatchi yoxud xaker turli xil kiberjinoyatlarni kompyuter orqali amalga oshiradi, bunga misol qilib onlayn firibgarlik turli xil sayt va tizimlarni buzishni keltiramiz, kompyuterga qarshi jinoyatlar – bunda jinoyatning asosiy maqsadi kompyuter tizimlari, dasturlar yoki ma’lumotlarga zarar yetkazish hisoblanadi. Bugungi kunda yurtimizda keng tarqalib borayotgan kiberjinoyat turi kopyuter va mobil telefonlar oraqali uyushtirilayotgan onlayn firibgarlik kiberjinoyatlardir.

Ushbu jinoyat turi birinchi marotaba Rossiya hudida aniqlangan, keyinchalik Belarusiya, Polsha, Ukarina va bugungi kunda O‘rta Osiyo mamalakatalridan Qozog‘iston, Qirg‘iziston va O‘zbekistonda avj oldi. Ushbu jinoyatning paydo bo‘lishiga yoxud avj olishiga aholining ijtimoiy va texnologik ong va madaniyatga e’tibosizliklari asosiy sabablardan biridir.

Tahlillarga ko‘ra, dunyo bo‘ylab har yili 500 milliondan ortiq kiber hujumlar uyushtiriladi. Har soniyada 12 nafar insondan biri kiber makonda sodir etilgan hujumlar qurboniga aylanadi. Amerika Qo‘shma Shtatlari, Fransiya, Angliya, Germaniya, Belgiya, Luksemburg kabi rivojlangan davlatlarda jinoyatlarning 60-65 foizi kiber hujumlar orqali sodir etilmoqda. O‘zbekistonda ham so‘nggi uch yilda bu

turdagi jinoyatlar 8,3 baravarga ko‘payib, hozirda umumiy jinoyatchilikning qariyb 5 foiziga yetgan. Xususan, noqonuniy bank-moliya operatsiyalari orqali o‘zgalarning plastik kartadagi mablag‘larini o‘zlashtirish, zararli viruslar tarqatish, qimor va tavakkalchilikka asoslangan onlayn o‘yinlar, diniy aqidaparastlikka qaratilgan axborot xurujlari, onlayn savdo maydonidagi firibgarlik jinoyatlari ko‘payib bormoqda.

Bugungi kunda kiberjinoyat jahon bo‘ylab shu qadar kuchayib ketdiki, hattoki qidiruv natijalariga ko‘ra O‘rta Osiyoning o‘zidayoq 40 dan ortiq kiberjinoiy guruhlar borligi aniqlangan, ularning 20 tasi bir necha yuz kishidan, ozroq qismi esa mingdan ortiq ekanligi aniqlangan. Bulardan tashqari jahon miqyosidagi yirik kiberjinoiy guruhlar ham mavjud, bunga misol qilib 2014-yil aniqlangan “Lazarus” gururhini olishimiz mumkin.

Ular shu yilda “SONY” kinokompaniyasiga kiberhujum uyushtirib hali kinoteatrlarga ham taqdim etilmagan 3 ta filmni internet orqali tarqatib yuborish natijasida kinokompaniyaga 3,2 million dollarlab zarar yetkazishadi. 2016-yil “Lazarus” xakerlar jamoasi yana qayta o‘zlarini namoyon etdilar. Bu galgi harakatda ular kattaroq “nishon”ga harakat qilishdi, ya’ni Bangladeshning asosiy moliyaviy organi Markaziy Bankiga. Ushbu hujum orqali ular 86000,000 dollar “foyda” qilishdi. Ammo shu kabi xakerlik hujumlarini oldini oladigan xalqaro “Kaspersky” laboratoriyasi tashkil etilgan va u ushbu hujumni takrorlanmasligi uchun Bangladesh Markaziy Bankiga kodli dasturlar yaratib berishdi. Qidiruv natijasida “Lazarus” xakerlar guruhi KXDR hududida ekanligi aniqlangan.

Bu kabi holatlar yurtimizda ham uchrab turibdi. Kiberfiribgarlarning odamalrning bank kartalaridan pul yechib olish holatlari natijasida bank kartalaridan yechib olingan mablag‘ 2022-yil ma’lumotlariga ko‘ra 1.676 mlrd. So‘mni tashkil etadi. Ushbu jinoyatningi atigi 12 foizini amalga oshirgan xakerlar qo'lga olingan, bu esa yuritimizda kiberjinoyatlarga qarshi kurash yetarli darajada rivojlanmagan ekanini ko'rsatadi.

Qo'lga olingan kibererfiribgarlar bergan ma'lumotlarga ko'ra ular o'z faoliyatini avvolo o'z “nishonlar”ini o'rganishdan boshlaydilar, ya'ni ular kim, nima bilan shug'ullanadi, yaqin insonlari va qarindoshlari haqida ma'lumot to'plashdan boshlashadi, bu shuni anglatadiki firibgarlarga aldanib qolgan shaxslarning aksariyat qismi ularning tanishlari yoxud unchalik ham ular uchun begonia bo'lmagan shaxslardir.

Keyingi bosqichda esa ular pulni qay tarzda aldab olish mumkinligi haqida ma'lumkt to'plashadi, ya'ni ular o'z pullarini kimga ishonib topshira olishadi yoxud kimlar uchun hech qanday o'y-hayollarsiz pullarini sarflay olishadi. Ushbu ma'lumotlarni qo'lga kiritishgach o'z “ mijozlar ”i bilan aloqaga chiqishadi va ularning yaqin insonlari bilan qandaydir noxush yangilik bo'lganini aytib ularga shu zahoti pul kerakligi haqida ma'lumot berishadi va ushbu holatdan shok holatiga tushgan jabrlanuvchi pulni yuborishini aytadi va pul yuborilishi kerak bo'lgan karta raqamini so'raydi, bunday holatda qo'lga tushishini bilgan jinoyatchilar ularga link yuborishadi vu pullarni shu link orqali yuborishlarini aytadi.

Shok holatidagi jabrlanuvchi hech narsaga e'tibor bermay link orqali o'z shaxsiy ma'lumotlari bo'lgan karta raqami va pinkodlarni kiritadi va shu ondayoq uning hisob raqamidagi barcha pullar yechib olinadi. Ushbu firibgarlik tuzog'iga asosan yoshi katta

insonlar osonlikcha aldanib qolishadi, bunga asosiy sabab esa ularning texnolgiya haqida to'laligicha ma'lumtga ega bo'lmasligidir. Ammo keyinchalik bank hisob raqamlari himoaysi anchayin kuchayib hatto hujum bo'lgan taqdirda ham hisob raqamdagi barcha pullarni yechib ololmaydigan darajaga keldi. Ammo bining “aqllilarimiz” bunga ham “yechim” topishdi.

Ular o'z jabrlanuvchilariga bank hodimi saifatida aloqaga chiqib uning bank hisob raqamiga hujum bo'layotgani haiqda yolg'on ma'lumot berishadi, natijada ularning hisob raqamidagi pullarni bir necha marotaba yechib olishadi. Ushbu jinoyat endigina paydo bo'lgan paytlarda bu usulga anchagina odamlar aldanishgandi, ammo zamon o'tgani saying odamlarda ham texnologik ong rivojlandi va ular bunga qayta ishinmay qo'yishdi, ammo kiberjinoyatchilar bu holatga ham tayyorgarlik ko'rib qo'yishgani ma'lum bo'ldi.

Ular endi telefon qo'ng'irog'I bilan emas, aksincha odamlar uchun ancha ishonchli bo'lgan manbalar ijtimliy tarmoqlardagi akkountlariga sun'iy intellekt yordamida a'loqaga chiqib sun'iy intellekt yordamida tayyorlangan video va audioxabarlar orqali aldashni boshlashdi. Bunday holatlar natijasida odamlarning deyarli 80 foiz qismi kartadan kartaga o'tkazamalrni deyarli amalga oshirishmay qo'yishdi, ular faqat bankomatlar orqali o'z hisob raqamlaridagi pullarni naqd pullarga aylantirib olishninma'qul ko'rishdi. Ammo Kiberjinoyatchilar bunga ham “yechim” topishdi.

Ular bankomatning karta qabul qilish qismlariga karta m'alumotlarini yozib oluvchi chiplar o'rnatishdi. Bank hodimlari buni tezda sezishdi va bankomatlaring ushbu qismiga antichiplar o'rnatishdi, ammo antichiplarning ki'rinishi chiplarning ko'rinishi bilan dayerli bir xil edi. Ushbu jinoyatlar kiberjinoyatchilarni qo'lga olish bilan va aholining texnologik ongi rivojlanishi natijasida bugungi kunda anchayin pasayib qoldi.

2024-yil ushbu jinoyatlarni qaytib takrorlanmasligi uchun bir qator islohotlar o'tkazildi.

Bular: O‘zbekistonning turli xil hududlarida aholiga aldanib qolmaslik uchun yo'l-yo'riqlar ko'rsatildi; kiberjinoyatning oldini olish uchun dasturlash bo'yicha chet eldan maxsus o'qituvchilar dasturchi talabalarga turli xil yangi metodlar o'rgatildi.

2024-yil noyabr oyida Buyuk Britaniya dasturchilari yangi sun'iy intellekt yaratildi va boshqalar. Kiberjinoyatlarni oldini olish uchun maxsus dasturlash kurslari yaratildi. Buyuk Britaniyada yaratilgan “ Neyro Buvi “ deb nomlangan sun'iy intellekt kiberfiribgarlar uchun haqiqiy “azoblash” bo'ldi. Chunki kiberfiribgarlarning asosiy jabrlanuvchilari yoshi katta, qariya insonlardir.

Kiberfiribgarlar asosan tarmoqda mavjud bo'lmagan raqamlardan foydalanib qo'ng'iroq qilishadi va bunday qo'ng'iroqlarni dastur avtomatik ravishda “Neyro Buvi” ga yo'nlatiradi, ushbu sun'iy intellekt ularga huddi hamma naesani to'liq tushunib turganday ma'lumot beradi va ularga kelgan sms kodlarni xato aytadi va ular bilan 40 daqiqagacha ular bilan mulaqot qilib ularning vaqtini o'g'irlaydi. Bu o'ylab topilgan usul anchagina jinoyatlarninoldini oldi va bizning yurtimizda ham keng qo'llanilsa jinoyatchilik foizi ancha tushgan bo'lardi.

Kiberjinoyatchilik zamonaviy dunyoda tez sur’atlar bilan rivojlanayotgan va jiddiy xavf tug‘dirayotgan hodisadir. Axborot texnologiyalari hayotimizning deyarli

barcha sohalariga chuqur kirib kelayotgan bir paytda, ushbu texnologiyalardan noqonuniy foydalanish ko‘plab ijtimoiy va iqtisodiy zararlarni keltirib chiqarmoqda. O‘zbekistonda ham so‘nggi yillarda bu jinoyatlar sezilarli darajada ko‘payib, global tendensiyalarga uyg‘un tarzda rivojlanmoqda. Maqolada keltirilgan ma’lumotlar shuni ko‘rsatadiki, kiberjinoyatchilikka qarshi kurashning nafaqat texnologik, balki ijtimoiy, huquqiy va psixologik aspektlarini ham hisobga olish zarur.

Kiberjinoyatchilikka qarshi kurash faqat texnologik choralar bilan cheklanib qolmasligi kerak. Bu jarayonni kengroq kontekstdan, ya’ni texnologik, ijtimoiy va huquqiy omillarni birgalikda hisobga olgan holda boshqarish lozim. O‘zbekistonning rivojlanayotgan texnologik infratuzilmasi va xalqaro tajribadan foydalanish imkoniyatlari bu borada katta ustunlik bo‘lib xizmat qilishi mumkin.

Ilmiy tadqiqotlar shuni ko‘rsatadiki, kiberjinoyatlarning aksariyati fuqarolarning texnologik savodxonlik darajasi pastligi tufayli amalga oshiriladi. Shu sababli, maktab va oliy ta’lim muassasalaridan boshlab, barcha yoshdagi aholiga zamonaviy texnologiyalardan xavfsiz foydalanish bo‘yicha bilim va ko‘nikmalarni singdirish lozim. Bunda innovatsion yondashuvlar, masalan, interaktiv kurslar va sun’iy intellekt asosida o‘quv dasturlaridan foydalanish samarali bo‘lishi mumkin.

Ilg‘or texnologiyalar, xususan sun’iy intellekt va “blockchain” texnologiyalari, kiberjinoyatlarning oldini olishda katta salohiyatga ega. Buyuk Britaniyada ishlab chiqilgan “Neyro Buvi” singari tizimlar O‘zbekistonda ham joriy qilinsa, kiberjinoyatchilarning faoliyati sezilarli darajada cheklanishi mumkin. Bu esa yurtimizda texnologik xavfsizlikni oshirishda ilmiy va amaliy qadamlar tashlash imkonini beradi.

Kiberjinoyatchilikning xalqaro xususiyatga ega ekanini hisobga olib, mamlakatlararo hamkorlikni kuchaytirish zarur. Xalqaro miqyosda qo‘shma dasturlar va loyihalarni amalga oshirish, kiberjinoyatchilikka qarshi kurash bo‘yicha global standartlarga mos keluvchi qonunchilikni takomillashtirish muhim ahamiyatga ega.

Kiberjinoyatchilikning yangi shakllarini aniqlash va ularga qarshi kurashish uchun fundamental va amaliy tadqiqotlarni kuchaytirish zarur. Bu borada milliy va xalqaro ilmiy jamoalarning o‘zaro hamkorligini ta’minlash va yosh olimlarni qo‘llab-quvvatlash kiberjinoyatlarga qarshi innovatsion yondashuvlarni ishlab chiqish imkonini beradi.

Muxtasar qili aytganda kiberjinoyatchilikka qarshi kurash – bu nafaqat davlat, balki jamiyatning har bir a’zosi ishtirok etishi zarur bo‘lgan kompleks jarayondir. Kiberxavfsizlikni ta’minlashda yuqori texnologiyalarni joriy qilish bilan bir qatorda, fuqarolarning texnologik savodxonligini oshirish va xalqaro hamkorlikni kuchaytirish muhim ahamiyatga ega. Faqat shunday yondashuv orqali biz zamonaviy texnologiyalar davrida xavfsiz va barqaror jamiyatni barpo etishimiz mumkin.

FOYDALINLIGAN ADABIYOTLAR

1. Vikipediya umumma'lumot sayti
2. Kun.uz axborot-ma'lumot sayti
3. Tishkent viloyati Adliya bishqarmasi statistik ma'lumotlar sayti

Shakurov R.R, Yuristlar malakasini oshirish markazi. Toshkent 2022-y

ЎЗБЕКИСТОНДА АХБОРОТ ВА КОМПЬЮТЕР ТИЗИМИДАН ФОЙДАЛАНИШ СОҲАСИДАГИ ҲУҚУҚБУЗАРЛИКЛАР УЧУН БЕЛГИЛАНГАН МАЪМУРИЙ ЖАВОБГАРЛИК

Хожиакбар Хусанович Бахрамов

Ўзбекистон Республикаси ИИВ Малака ошириш институти юридик фанлар кафедраси доценти

Аннотация. Мақолада ахборот ва компьютер тизимидан фойдаланиш соҳасидаги ҳуқуқбузарликлар, уларнинг турлари, энг кўп содир этиладиган кўринишлари ҳамда уларни олдини олиш ва қарши курашиш масалалари ёритилган.

Калит сўзлар: ахборот технологиялари, ахборот ва компьютер тизимидан фойдаланиш соҳасидаги ҳуқуқбузарликлар, ахборот ва компьютер тизимидан фойдаланиш соҳасидаги ҳуқуқбузарликлар учун белгиланган маъмурий жавобгарлик.

Аннотация. В статье рассматриваются правонарушения в сфере использования информационных и компьютерных систем, их виды, наиболее распространенные проявления, а также вопросы предупреждения и борьбы с ними.

Ключевые слова: информационные технологии, правонарушения в сфере использования информационных и компьютерных систем, административная ответственность за правонарушения в сфере использования информационных и компьютерных систем.

Annotation. The article discusses offenses in the use of information and computer systems, their types, the most common manifestations, as well as issues of prevention and control.

Keywords: information technologies, offenses in the use of information and computer systems, administrative liability for offenses in the use of information and computer systems.

Жаҳонда бўлгани каби юртимизда ҳам ахборот-коммуникация технологияларининг ўрни тобора ортиб бораётгани, зарур ахборотлардан тезкор хабардор бўлиш, турли интерактив хизматлардан фойдаланиш имконини яратади. Бу эса, республикамиздаги турли корхона, ташкилот ва муассасаларда фаолият олиб борадиган ходим ва хизматчиларнинг шу жумладан, фуқароларимизнинг замонавий ахборот-коммуникация технологияларидан самарали фойдаланишларига кенг имконият. Зеро, глобал тараққиёт шароитида ҳар бир инсон ҳам ахборот-коммуникация технологияларидан унумли фойдаланиш ҳуқуқига эга. Янги таҳрирда қабул қилиги Чунки, уларнинг кунлик ҳаёт фаолиятида амалга оширадиган ишларида компьютер техникасидан, тармоқ технологияларидан унумли фойдаланишлари уларнинг иш сифатини ортиши, сарфланадиган вақтни тежаш имконини беради.

Шу боис, мамлакатимизда компьютер ва ахборот технологиялари, телекоммуникация ва маълумот узатиш тармоқлари, интернет хизматларини ривожлантириш ҳамда замонавийлаштириш муҳим ва асосий йўналишлардан бири. Ушбу йўналишда уларни жаҳон стандартларига етказиш мақсадида кенг кўламли ишлар амалга оширилмоқда.

Мазкур мақсад ва натижаларга эришиш ҳамда бу борадаги ижтимоий муносабатларни тартибга солиш учун республикамизда зарур меъёрий-ҳуқуқий асослар яратилган жумладан, Ўзбекистон Республикасининг “Алоқа тўғрисида”ги, “Почта алоқаси тўғрисида”ги, “Телекоммуникациялар тўғрисида”ги, “Ахборотлаштириш тўғрисида”ги, “Электрон рақамли имзо тўғрисида”ги, “Электрон ҳужжат айланиши тўғрисида”ги, “Электрон тижорат тўғрисида”ги, “Электрон ҳукумат тўғрисида”ги, “Киберхавфсизлик тўғрисида”ги қонунлар ҳамда Ўзбекистон Республикаси Президентининг бир қанча фармонлари, ҳукумат қарорлари қабул қилинган. Шунингдек, фаол ривожланиб бораётган бозор муносабатлари шароитида ушбу меъёрий-ҳуқуқий асослар янада такомиллаштирилиб борилмоқда.

Бугунги шароитда, интернет ва электроника даврида иқтисодиёт тармоқларида замонавий ахборот-коммуникация технологияларини кенг жорий этиш, “Электрон ҳукумат” тизими фаолиятини янада ривожлантириш устувор аҳамиятга эгадир. Жаҳон тажрибаси шундан далолат берадики, айни пайтда глобал иқтисодиётда компьютер ва телекоммуникация технологиялари, дастурий таъминот маҳсулотларини ишлаб чиқариш ва улар асосида кенг турдаги интерфаол хизматлар кўрсатишни ўз ичига олган ахборот-коммуникация технологиялари соҳасининг роли ва аҳамияти тобора ортиб бормоқда.

Ахборот-коммуникация технологияларининг ривожланиши мамлакатнинг рақобатдошлик даражасига таъсир кўрсатиши, катта ҳажмда ахборот тўплаш ва уни умумлаштириш имконини бериши, бошқаришни стратегик даражада ташкил этиш учун кенг имкониятлар очиб беришини унутмаслигимиз зарур, ахборот-коммуникация технологияларининг мамлакатимизни ижтимоий-иқтисодий ривожланишида тутган ўрни муҳим аҳамият касб этади.

Мазкур фикрлардан келиб чиқиб шуни таъкидлаш керакки, бу соҳада яратилган имкониятлар ҳуқуқ ва эркинликлар ҳамда ижтимоий муносабатларга тажовуз қилиниши яъни юқорида қайд этилган қонунлар талабларининг бузилиши – ҳуқуқбузарлик содир этилиши ҳисобланади.

Ўзбек тилининг изоҳли луғатида компьютер (инг. computer, лотинча computare – ҳисобламоқ, ҳисоблаб чиқмоқ маъноларини билдиради) Мураккаб қурилмага эга бўлган электрон ҳисоблаш машинасидир.

Амалдаги Маъмурий жавобгарлик тўғрисидаги кодекснинг 10-моддасига асосан маъмурий жавобгарлик тўғрисидаги қонунчиликка биноан маъмурий жавобгарликка тортиш назарда тутилган, шахсга, фуқароларнинг ҳуқуқлари ва эркинликларига, мулкчиликка, давлат ва жамоат тартибига, табиий муҳитга тажовуз қилувчи ғайриҳуқуқий, айбли (қасддан ёки эҳтиётсизлик орқасида) содир этилган ҳаракат ёки ҳаракатсизлик маъмурий ҳуқуқбузарликдир.

Ушбу ҳуқуқбузарлик учун маъмурий жавобгарлик, башарти бу ҳуқуқбузарлик ўз хусусиятига кўра жиноий жавобгарликка тортишга сабаб бўлмаган тақдирда, қўлланилади.

Ҳуқуқбузарликнинг иккинчи тури яъни жиноят (жиноий ҳуқуқбузарлик) маъмурий ҳуқуқбузарликдан ижтимоий хавфлилиги ҳамда шахснинг содир этган жинояти учун ҳукм этилганида юзага келадиган судланганлик ҳуқуқий ҳолати билан фарқ қилади.

Ўзбекистон Республикасининг Жиноят кодексининг 14 моддасига биноан ушбу кодекс билан тақиқланган, айбли ижтимоий хавфли қилмиш (ҳаракат ёки ҳаракатсизлик) жазо қўллаш таҳдиди билан жиноят деб топилади. Жиноят кодекси билан қўриқланадиган объектларга зарар етказадиган ёки шундай зарар етказиш реал хавфини келтириб чиқарадиган қилмиш ижтимоий хавфли қилмиш деб топилади.

Ахборот тизими, ва компьютер тизимидан, телекоммуникация тармоғидан қонунга хилоф равишда фойдаланиш, крипто-активлар айланмаси соҳасидаги қонунчиликни бузиш, майнинг фаолиятини қонунга хилоф равишда амалга ошириш каби белгиланган тартиб қоидаларини бузганлик учун Маъмурий жавобгарлик тўғрисидаги кодекснинг Махсус қисми 11-боби 155–155^5-моддаларида (жами 6та моддада) маъмурий жавобгарлик белгиланган.

Жумладан, кодекснинг 155-моддаси “Ахборотдан фойдаланиш қоидаларини бузиш” деб номланган бўлиб ушбу модда тўрт қисмдан иборат бўлиб қуйидаги ғайриҳуқуқий қилмишлар учун маъмурий жавобгарликни назарда тутади.

Ахборот тизимидан фойдаланиш мақсадида унга рухсатсиз кириб олишда ифодаланган ахборот ва ахборот тизимларидан фойдаланиш қоидаларини бузиш – фуқароларга базавий ҳисоблаш миқдорининг учдан бир қисмидан бир бараваригача, мансабдор шахсларга эса – бир бараваридан уч бараваригача миқдорда жарима солишга сабаб бўлади.

Ахборот тизимларининг ишини бузишга олиб келган худди шундай ҳуқуқбузарлик, худди шунингдек кириш чекланган ахборот тизимларини ахборот-ҳисоблаш тармоқларига улаш чоғида тегишли ҳимоя чораларини кўрмаганлик – фуқароларга базавий ҳисоблаш миқдорининг бир бараваридан уч бараваригача, мансабдор шахсларга эса – уч бараваридан беш бараваригача миқдорда жарима солишга сабаб бўлади.

Юридик ва жисмоний шахсларнинг ахборот тизимларини халқаро ахборот тармоқларига қонунга хилоф равишда улаш, бу тармоқларга тегишли ҳимоя чораларини кўрмасдан уланиш, худди шунингдек улардан маълумотларни қонунга хилоф равишда олиш – фуқароларга базавий ҳисоблаш миқдорининг икки бараваридан беш бараваригача, мансабдор шахсларга эса – беш бараваридан етти бараваригача миқдорда жарима солишга сабаб бўлади.

Ўзганинг электрон ҳисоблаш машиналари учун яратилган дастури ёки маълумотлар базасини ўз номидан чиқариш ёхуд қонунга хилоф равишда ундан нусха олиш ёки бундай асарларни тарқатиш – фуқароларга базавий ҳисоблаш миқдорининг бир бараваридан уч бараваригача, мансабдор шахсларга эса – уч бараваридан беш бараваригача миқдорда жарима солишга сабаб бўлади.

Мазкур ҳуқуқбузарликнинг юридик таркибини қуйидагича ифодалаш мумкин. Ҳуқуқбузарликнинг объекти – алоқа, ахборот ва ахборот тизимидан фойдаланиш соҳасидаги қонун билан қўриқланадиган ижтимоий муносабатлардир.

Ҳуқуқбузарликнинг объектив томони – ғайриҳуқуқий ҳаракат шунингдек ҳаракатсизликда ифодаланадиган қилмишлардир. Жумладан, ушбу модданинг биринчи ва тўртинчи қисмларида назарда тутилган қилмишлар ғайриҳуқуқий ҳаракат орқали содир этилади. 155-модданинг иккинчи ва учинчи қисмларида назарда тутилган қилмишлар ғайриҳуқуқий ҳаракат билан ҳам ҳаракатсизлик билан ҳам содир этилиши мумкин.

Ҳуқуқбузарликнинг субъектив томони – қасддан ҳам эҳтиётсизлик орқасида ҳам содир этилиши мумкин бўлган қилмишлардир.

Ҳуқуқбузарликнинг субъекти – 16 ёшга тўлган жисмоний шахслар шунингдек мансабдор шахслар ҳам жавобгарликка тортилиши мумкин.

Мазкур ҳуқуқбузарликни Жиноят ишлари бўйича судлар кўриб чиқиб жазо қўллаш тўғрисида қарор қабул қиладилар.

Маъмурий жавобгарлик тўғрисидаги кодекснинг 155^1-моддаси Компьютер тизимидан фойдаланиш қоидаларини бузиш деб номланган бўлиб ушбу модда икки қисмдан иборат бўлиб қуйидаги ғайриҳуқуқий қилмишлар учун маъмурий жавобгарликни назарда тутади.

Компьютер тизимидан фойдаланишга рухсати бўлган шахснинг ушбу тизимдан фойдаланишнинг белгиланган қоидаларини бузиши компьютер ахборотининг йўқ қилиб юборилишига, тўсиб қўйилишига, модификациялаштирилишига, компьютер ускунаси ишлашининг бузилишига сабаб бўлса, – фуқароларга базавий ҳисоблаш миқдорининг беш бараваридан етти бараваригача, мансабдор шахсларга эса – етти бараваридан ўн бараваригача миқдорда жарима солишга сабаб бўлади.

Худди шундай ҳуқуқбузарлик конфиденциал ахборот мавжуд бўлган компьютер тизимидан фойдаланиш вақтида содир этилса, – фуқароларга базавий ҳисоблаш миқдорининг етти бараваридан ўн бараваригача, мансабдор шахсларга эса – ўн бараваридан ўн беш бараваригача миқдорда жарима солишга сабаб бўлади.

Мазкур ҳуқуқбузарликнинг юридик таркиби қуйидагича бўлиши мумкин. Ҳуқуқбузарликнинг объекти – ахборот ва компьютер тизимидан фойдаланиш соҳасидаги қонун билан қўриқланадиган ижтимоий муносабатлардир.

Ҳуқуқбузарликнинг объектив томони – модданинг биринчи, иккинчи қисмида ҳам ғайриҳуқуқий ҳаракат билан содир этиладиган қилмишлардир.

Ҳуқуқбузарликнинг субъектив томони – қасддан содир этилиши мумкин бўлган қилмишлардир.

Ҳуқуқбузарликнинг субъекти сифатида – компьютер тизимидан фойдаланишга рухсати бўлган шахс шунингдек мансабдор шахс ҳам жавобгарликка тортилиши мумкин.

Маъмурий жавобгарлик тўғрисидаги кодекснинг 155^2-моддаси “Телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш” деб номланган бўлиб ушбу модда бир қисмдан иборат бўлиб

қуйидаги ғайриҳуқуқий қилмишлар учун маъмурий жавобгарликни назарда тутади. Телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш, жиноят аломатлари мавжуд бўлмаган тақдирдагина – ҳуқуқбузарлик содир этиш қуролини мусодара қилиб, фуқароларга базавий ҳисоблаш миқдорининг ўн бараваридан йигирма бараваригача, мансабдор шахсларга эса – йигирма бараваридан эллик бараваригача миқдорда жарима солишга сабаб бўлади.

Сир эмаски, сўнги йилларда мамлакатимизда барча соҳаларда ахборот-коммуникация технологияларини жорий этишга қаратилган кенг кўламли ислоҳотлар амалга оширилди ва жадаллик билан давом эттирилмоқда.

Аммо, айрим шахслар томонидан замонавий рақамли технологиялар ютуқларидан қонунга хилоф равишда ҳамда ғаразли мақсадларда фойдаланилиши натижасида фуқароларнинг ҳуқуқлари ва қонуний манфаатлари бузилаётганлиги ҳамда давлатга зарар етказилаётганлиги боис. Бу рақамли технологиялардан фойдаланган ҳолда содир этилаётган янги турдаги ҳуқуқбузарликлар ва жиноятлар учун жавобгарлик белгиланишини тақозо этганлиги сабабли Қонун чиқарувчи ҳокимият томонидан 2024 йил 19 январда Ўзбекистон Республикасининг “Ўзбекистон Республикасининг Жиноят, Жиноят-процессуал кодексларига ҳамда Ўзбекистон Республикасининг Маъмурий жавобгарлик тўғрисидаги кодексига ўзгартириш ва қўшимчалар киритиш ҳақида”ги ЎРҚ-899-сонли Қонунига асосан Маъмурий жавобгарлик тўғрисидаги кодексининг мазкур 11-Бобига “мобиль қурилманинг халқаро ўзига хос идентификация кодини ёки абонент қурилмасининг идентификациялаш модулини қонунга хилоф равишда ўзгартирганлик, крипто-активлар айланмаси соҳасидаги қонунчиликни бузганлик ва майнинг фаолиятини қонунга хилоф равишда амалга оширганлик учун маъмурий жавобгарликни назарда тутувчи қуйидаги янги 155^3-, 155^4- ва 155^5-моддалар киритилиб” маъмурий жавобгарлик белгиланди.

Уларни таҳлил қиладиган бўлсак, Маъмурий жавобгарлик тўғрисидаги кодекснинг 155^3-моддаси “Мобиль қурилманинг халқаро ўзига хос идентификация кодини ёки абонент қурилмасининг идентификациялаш модулини қонунга хилоф равишда ўзгартириш” деб номланган бўлиб ушбу модда икки қисмдан иборат бўлиб қуйидаги ғайриҳуқуқий қилмишлар учун маъмурий жавобгарликни назарда тутади.

1-қисми бўйича “Мобиль қурилманинг халқаро ўзига хос идентификация кодини қонуний ишлаб чиқарувчининг рухсатисиз ўзгартириш, худди шунингдек ушбу мақсадда махсус дастурларни ишлаб чиқиш, тарқатиш ёки улардан фойдаланганлик” – ҳуқуқбузарлик содир этиш қуролини мусодара қилиб, базавий ҳисоблаш миқдорининг ўн беш бараваридан йигирма бараваригача миқдорда жарима солишга сабаб бўлади.

2-қисми бўйича “Абонент қурилмасининг идентификациялаш модулини қонуний ишлаб чиқарувчининг ёки унинг қонуний эгасининг рухсатисиз ўзгартириш ёки унинг нусхасини яратиш, – ҳуқуқбузарлик содир этиш қуролини мусодара қилиб, базавий ҳисоблаш миқдорининг йигирма бараваригача миқдорда жарима солишга сабаб бўлади.

Кодекснинг 155[4]-моддаси “Крипто-активлар айланмаси соҳасидаги қонунчиликни бузиш” деб номланган бўлиб ушбу модда ҳам икки қисмдан иборат бўлиб қуйидаги ғайриҳуқуқий қилмишлар учун маъмурий жавобгарликни назарда тутади.

1-қисми бўйича “Крипто-активларни қонунга хилоф равишда олиш, ўтказиш ёки айирбошлаш, белгиланган тартибда лицензия олмасдан крипто-активлар айланмаси соҳасидаги хизматлар провайдерлари фаолиятини амалга ошириш, – крипто-активларни ҳамда мазкур ҳуқуқбузарликларни содир этиш қуролларини мусодара қилиб, ўн беш суткагача маъмурий қамоққа олишга ёки МЖтКга мувофиқ ўзига нисбатан маъмурий қамоқ қўлланилиши мумкин бўлмаган шахсларга базавий ҳисоблаш миқдорининг йигирма бараваридан ўттиз бараваригача миқдорда жарима солишга сабаб бўлади.

2-қисми бўйича “Крипто-активлар айланмаси соҳасидаги хизматлар провайдерлари томонидан аноним крипто-активлар билан операцияларни амалга ошириш, – мансабдор шахсларга базавий ҳисоблаш миқдорининг ўттиз бараваридан қирқ бараваригача миқдорда жарима солишга сабаб бўлади.

Мазкур қилмишлар қасддан қилинадиган хатти-ҳаракатлар ҳисобланиб, модданинг 2-қисмида назарда тутилган қилмишлар учун фақат мансабдор шахслар жавобгарликка тортилиши белгиланган.

Кодекснинг 155[5]-моддаси “Майнинг фаолиятини қонунга хилоф равишда амалга ошириш” деб номланган бўлиб ушбу модда тўрт қисмдан иборат бўлиб қуйидаги ғайриҳуқуқий қилмишлар учун маъмурий жавобгарликни назарда тутади.

1-қисми бўйича “Майнинг фаолиятини белгиланган тартибни бузган ҳолда амалга ошириш, – мазкур ҳуқуқбузарликни содир этиш қуролларини мусодара қилиб, беш суткагача маъмурий қамоққа олишга ёки ушбу Кодексга мувофиқ ўзига нисбатан маъмурий қамоқ қўлланилиши мумкин бўлмаган шахсларга базавий ҳисоблаш миқдорининг йигирма бараваридан ўттиз бараваригача миқдорда жарима солишга сабаб бўлади.

2-қисми бўйича “Аноним крипто-активлар майнинги билан шуғулланиш, – крипто-активларни ҳамда ҳуқуқбузарлик содир этиш қуролларини мусодара қилиб, мансабдор шахсларга базавий ҳисоблаш миқдорининг ўттиз бараваридан қирқ бараваригача миқдорда жарима солишга сабаб бўлади.

3-қисми бўйича “Мазкур модданинг биринчи қисмида назарда тутилган ҳуқуқбузарликни анча миқдорда содир этганлик учун, – мазкур ҳуқуқбузарликни содир этиш қуролларини мусодара қилиб, ўн суткагача маъмурий қамоққа олишга ёки МЖтКга мувофиқ ўзига нисбатан маъмурий қамоқ қўлланилиши мумкин бўлмаган шахсларга базавий ҳисоблаш миқдорининг ўттиз бараваридан эллик бараваригача миқдорда жарима солишга сабаб бўлади.

4-қисмида эса “Ушбу модданинг биринчи қисмида назарда тутилган ҳуқуқбузарликни кўп миқдорда содир этганлик учун, – мазкур ҳуқуқбузарликни содир этиш қуролларини мусодара қилиб, ўн беш суткагача маъмурий қамоққа олишга ёки МЖтКга мувофиқ ўзига нисбатан маъмурий қамоқ қўлланилиши мумкин бўлмаган шахсларга базавий ҳисоблаш миқдорининг эллик бараваридан юз бараваригача миқдорда жарима солишга сабаб бўлиши белгиланди.

Маъмурий жавобгарлик тўғрисидаги кодекснинг 245 моддасига биноан мазкур ҳуқуқбузарликни Жиноят ишлари бўйича судлар кўриб чиқиб жазо қўллаш тўғрисида қарор қабул қиладилар.

Юқорида кўриб чиқилган масалалардан келиб чиқиб шуни таъкидлаш керакки, мамлакатимизда ахборот ва компьютер тизимидан фойдаланиш соҳасидаги ижтимоий муносабатлар норматив-ҳуқуқий жиҳатдан тўлиқ ҳуқуқий тартибга солинган ҳамда маъмурий ва жиноий-ҳуқуқий жиҳатдан муҳофазаланган.

Шу боис, жамиятимизнинг барча аъзолари мазкур қонун ҳужжатларининг моҳияти ва талабларини тушуниши, ўрганиши ҳамда энг аввало уларнинг талабларига риоя этишлари муҳим аҳамият касб этади.

Фойдаланилган адабиётлар рўйхати.

4. Ўзбекистон Республикаси Конституцияси. (Янги таҳрирда) 2023 йил 30 апрель.
5. Ўзбекистон Республикасининг “Киберхавсизлик тўғрисида”ги ЎРҚ-764-сон қонуни. 2022 йил 15 апрель.
6. Ўзбекистон Республикасининг Маъмурий жавобгарлик тўғрисидаги кодекси. Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси. 1995. 1-сон.
7. Ўзбекистон Республикасининг Жиноят кодекси. Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси. 1995. 1-сон.
8. Ўзбекистон Республикасининг 2024 йил 19 январдаги ЎРҚ-899-сонли қонуни. Қонунчилик маълумотлари миллий базаси, 19.01.2024 й., 03/24/899/0048-сон.

M U N D A R I J A

O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti

KIBERJINOYATCHILIKKA QARSHI KURASHISHNING HUQUQIY, TASHKILIY, MOLIYAVIY-IQTISODIY, MUHANDISLIK-TEXNIK MUAMMOLARI VA YECHIMLARI

Respublika ilmiy-amaliy konferensiya materiallari to‘plami

Toshkent 2024-yil 5-dekabr

Bosishga ruxsat etildi 13.12.2024-y. Nashriyot-hisob tabog‘i 18. Adadi 10-nusxa. Buyurtma №___. Bahosi shartnoma asosida

O‘zbekiston Respublikasi IIV Malaka oshirish instituti, 100213. Toshkent shahar. Husayn Boyqaro ko‘chasi, 27a-uy.