



ARTICLE INFO

Received: 14th January 2023

Accepted: 23th January 2023

Online: 24th January 2023

KEY WORDS

Ахборот, ахборот-коммуникация технология, кибер, хавфсизлик, компьютер, жиноят.

**АХБОРОТ ХАВФСИЗЛИГИ ҲАМДА МУҲОФАЗАСИ
ТАЪМИНЛАНГАНИГА ҚАРАМАСДАН СОДИР
ЭТИЛАДИГАН ЖИНОЯТЛАР**

Ғаниев Фаррух Тахиржанович

Ўзбекистон Республикаси ИИВ Академияси

Ҳуқуқбузарликлар профилактикаси ва

криминология кафедраси ўқитувчиси

fargan77@bk.ru

<https://doi.org/10.5281/zenodo.7565123>

ABSTRACT

Мақолада ахборот хавфсизлиги ҳамда муҳофазаси таъминланганига қарамасдан содир этиладиган жиноятлар бўйича батафсил таҳлилий маълумотлар ёртилган. Ахборот-коммуникация технология соҳасида киберхавфсизликни таъминлаш масалаларни кўриб чиқилган. Ахборот технологиялари соҳасидаги жиноятлар содир бўлиш сабаблари ўрганилган.

Ахборотни ҳимоялаш технологияси ахборотларга бўлган хавфлар ахборот хавфсизлиги тизимлари компьютер вируси ва унинг турлари.

Ахборот хавфсизлигини таъминлаш. Ахборот хавфсизлигини таъминлаш – бу фойдаланувчининг ахборотларини ҳимоялашга қўйилган меъёр ва талабларни бажаришидир. Ахборот хавфсизлиги эса бу ахборот фойдаланувчиларига ва кўплаб ахборот тизимларига зарар келтирувчи табиий ёки сунъий характерга эга тасодифий ва уюштирилган таъсирлардан ахборотларни ва ахборот коммуникация тизим объектларининг ҳимояланганлигидир.

Логин тушунчаси. Логин – шахснинг, ўзини ахборот коммуникация тизимига таништириш жараёнида қўлланиладиган белгилар кетма-кетлиги бўлиб, ахборот коммуникация тизимидан фойдаланиш ҳуқуқига эга бўлиш учун фойдаланувчининг махфий бўлмаган қайд ёзуви ҳисобланади.

Парол тушунчаси. Парол – унинг эгаси ҳақиқийлигини аниқлаш жараёнида текширув ахбороти сифатида ишлатиладиган белгилар кетма-кетлиги. У компьютер билан мулоқот бошлашдан олдин, унга клавиатура ёки идентификация картаси ёрдамида киритиладиган ҳарфли, рақамли ёки ҳарфли-рақамли код шаклидаги махфий сўздан иборат.

Авторизация тушунчаси. Авторизация – фойдаланувчининг ресурсдан фойдаланиш ҳуқуқлари ва рухсатларини текшириш жараёни. Бунда фойдаланувчига ҳисоблаш тизимида баъзи ишларни бажариш учун муайян ҳуқуқлар берилади. Авторизация шахс ҳаракати доирасини ва у фойдаланадиган ресурсларни белгилайди. Рўйхатдан ўтиш тартиби. Рўйхатдан ўтиш – фойдаланувчиларни рўйхатга олиш ва уларга дастурлар ва маълумотларни ишлатишга ҳуқуқ бериш жараёни. Айрим веб-сайтлар фойдаланувчиларга қўшимча хизматларни олиш ва пуллик хизматларга обуна бўлиш учун рўйхатдан ўтишни, яъни ўзи ҳақида айрим маълумотларни киритишни (анкета



тўлдиришни) ҳамда логин ва парол олишни таклиф қиладилар. Фойдаланувчи рўйхатдан ўтгандан сўнг тизимда унга қайд ёзуви (account) яратилади ва унда фойдаланувчига тегишли ахборотлар сақланади.

Логин ва паролга эга бўлиш шартлари. Бирор шахс ўзининг логин ва паролига эга бўлиши учун у биринчидан ахборот коммуникация тизимида рўйхатдан ўтган бўлиши керак ва шундан сўнг у ўз логини ва паролини ўзи ҳосил қилиши ёки тизим томонидан берилган логин паролга эга бўлиши мумкин. Логин ва пароллар маълум узунликдаги белгилар кетма-кетлигидан ташкил топади. Логин ва паролларнинг узунлиги ва қийинлиги унинг қанчалик хавфсизлигини яъни бузиб бўлмаслигини таъминлайди. Логин ва паролни бузиш. Логин ва паролни бузиш – бу бузғунчининг бирор бир мақсад йўлида ахборот коммуникация тизими объектларидан фойдаланиш учун қонуний тарзда фойдаланувчиларга тегишли логин ва паролларини бузишдир. Бунда махсус дастур ёрдамида логин ва пароллар генерация қилиб топилади. Логин ва паролларнинг узунлиги бу жараённинг узоқ вақт давом этишига ёки генерация қилаолмасилигига ишора бўлади.

Логин ва паролни ўғирлаш. Логин ва паролни ўғирлаш – бу фойдаланувчиларнинг махфий маълумотлари бўлган логин ва паролларга эга бўлиш мақсадида амалга ошириладиган интернет фирибгарлигининг бир туридир. Бу машҳур брендлар, масалан, ижтимоий тармоқлар, банклар ва бошқа сервислар номидан электрон хатларни оммавий жўнатиш йўли орқали амалга оширилади. Хатда одатда ташқи кўриниши асл сайтдан фарқ қилмайдиган сайтга тўғри ишорат мавжуд бўлади. Бундай сайтга ташриф буюрган фойдаланувчи фирибгарга аккаунтлар ва банк ҳисоб рақамларига кира олишга эга бўлишга имкон берувчи муҳим маълумотларни билдириши мумкин. Фишинг – ижтимоий инженериянинг бир тури бўлиб, фойдаланувчиларнинг тармоқ хавфсизлиги асосларини билмаслигига асосланган. Жумладан, кўпчилик оддий фактни билишмайди: сервислар қайд ёзувингиз маълумотлари, парол ва шу каби маълумотларни юборишни сўраб ҳеч қачон хат юбормайди.

Ресурслардан рухсатсиз фойдаланиш ва унинг оқибатлари. Ахборот-коммуникация тизимининг ихтиёрий таркибий қисмларидан бири бўлган ҳамда ахборот тизими тақдим этадиган имконият мавжуд бўлган ресурслардан белгиланган қоидаларга мувофиқ бўлмаган ҳолда фойдаланишни чеклаш қоидаларига риоя қилмасдан фойдаланиш – бу ресурслардан рухсатсиз фойдаланиш тоифасига киради. Бундай фойдаланиш натижасида қуйидаги оқибатлар юзага келиши мумкин:

- ахборотнинг ўғирланиши;
- ахборотни ўзгартириш;
- ахборотнинг йўқотилиши;
- ёлғон ахборотни киритиш;
- ахборотни қалбакилаштириш ва ҳ.к.

Ахборот технологияларидан фойдаланган ҳолда содир этиладиган жиноятлар деб, *ахборот-коммуникация технологиялари воситаларидан фойдаланган ҳолда, виртуал тармоқда фойдаланувчиларни кўрқитиш, вирус ва бошқа зарарли дастурлар, қонунга зид ахборотлар тайёрлаш ва тарқатиш (spam), хакерлик хужуми, веб-сайтларга*



ноқонуний кириш, фирибгарлик, маълумотлар бутунлиги ва муаллифлик ҳуқуқини бузиш, кредит карточкалар рақами ҳамда банк реквизитларини ўғирлаш (фишинг ва фарминг) ва бошқа турли ҳуқуқбузарликлар тушунилади [1].

Ўзбекистон Республикаси Президентти Шавкат Мирзиёев Олий Мажлиснинг Сенати ва Қонунчилик палатасига навбатдаги Мурожаатномасида илм-маърифат ва технологиялар ривожига алоҳида аҳамият қаратди. Президентимиз таъкидлаганидек, «энг катта бойлик – бу ақл-заковат ва илм, Энг катта мерос – бу яхши тарбия, энг катта қашшоқлик – бу билимсизликдир! Шу сабабли ҳаммамиз учун замонавий билимларни ўзлаштириш, чинакам маърифат ва юксак маданият эгаси бўлиш, узлуксиз ҳаётий эҳтиёжга айланиши керак» [2].

Ахборот технологиялари соҳасидаги жиноятларнинг кўпайиши, уларнинг юқори даражадаги ижтимоий хавфлилиги мазкур жиноятлардан муҳофаза қилиш чораларини (аввало компьютер технологияларининг ўзини қўриқлаш орқали) ишлаб чиқишни тақозо этди. Тадқиқотларда кўрсатишича, бундай муҳофаза воситаларнинг 60% – ҳуқуқий воситаларга, 20% – криптографик ва 20% – дастурий, аппаратга оид ҳамда бошқа жисмоний, ташкилий воситаларга тўғри келади.

Ушбу жиноятлардан кўрилатган зарар ҳам бошқа мулкӣ жиноятлардан етадиган зарар миқдоридан анча юқоридир. Экспертларнинг маълумотларига асосан дунё бўйича мазкур турдаги жиноятлардан кўрилатган зарар миқдори йилига тахминан 200 млрд. АҚШ долларини ташкил қилади. Агар банкни “ўмармоқчи” бўлган шахс 10 минг АҚШ доллари учун ҳаётини гаровга қўйса, хаккер ҳеч қандай хавфсиз арзимаган вақт ичида бир миллиондан ортиқ пул маблағига эга бўлиши мумкин.

Ахборот технологиялари соҳасида содир этилаётган жиноятларнинг сабабларидан бири – бу юқори технологиялари билан боғлиқ муносабатларни самарали тартибга солишдаги камчиликларни эътироф этиш мумкин. Интернет тармоқлари ўзининг кенгмиқёслилиги, функциявийлиги, анонимлиги, аҳолининг муайян қисмининг технологик билимларининг етарли эмаслиги туфайли ҳам кучайиб боради.

Бугунги кунда хакерлар кун сайин кўпайиб бормоқда. Масалан маълумотларга кўра, Россиянинг кибержиноятлар бозоридаги хакерларнинг даромадлари бир йилда бир миллиард АҚШ долларидан кўпни ташкил қилган.

Хакерларнинг энг даромадли операциялари – бу турли компьютер фойдаланувчиларига ахборотлар юбориш, махфий маълумотларни ўғирлаш, Ddos дастури орқали фойдаланувчиларга хужум қилиш ва сайтларга тўсиқ қўйиш билан боғлиқ.

Шунингдек зарар етказувчи дастурларнинг сони аввалги йилларга нисбатан бир неча баробарга ортган. Интернетдан фойдаланувчилар мунтазам равишда кибер хужумларнинг қурбонлари бўладилар. Ўтган йили куррамизда истиқомат қилувчи ҳар бир кишига жами 5000дан ортиқ зарар етказувчи электрон ҳатлар келиб тушган ҳамда кибер жиноятчилар томонидан электрон ҳисоб-варақларни бузишга уринишлар қайд этилган.

Ижтимоий тармоқлар аллақачон жиноятчилар учун маълумотлар манбаига айланиб улгурган. Буюк Британияда ўтказилган тадқиқотларнинг натижаларига кўра, мулкка



қарши жиноятларнинг бешдан тўрт қисми Twitter и Facebookдаги маълумотларидан фойдаланган ҳолда содир этилган.

Ижтимоий тармоқлардаги шахсий варақлар бегона фойдаланувчиларга шахсга оид муҳим маълумотларни олишга имкон яратади. Кўп инсонлар ўзларининг ижтимоий варақларида автомашинаси, техник жиҳозлари, қимматбаҳо заргарлик буюмлари ва бошқалар тўғрисидаги фотосуратларни намойиш қиладилар. Бу эса жиноятчиларга жиноят қурбонларини танлаш имконини беради. Замонавий ахборот технологияларининг ривожланиши натижасида вужудга келган ҳамда бугунги кунда кенгайиб бораётган жиноят турларидан бири ҳисобланади. Ўзбекистон Республикаси Жиноят кодекси ушбу соҳада қуйидаги ҳаракатларни (ҳаракатсизликни) жиноят деб белгилайди:

- ахборотлаштириш қоидаларини бузиш (278¹-модда)
- компьютер ахборотига қонунсиз (руҳсатсиз) кириш (278²-модда)
- компьютер тизимига қонунсиз киришни таъминловчи махсус воситаларни сотиш мақсадида тайёрлаш ёки сотиш ва тарқатиш (278³-модда)
- компьютер ахборотларини модификациялаш (278⁴-модда)
- компьютерни ишдан чиқариш (278⁵-модда)
- зарар етказувчи дастурларни яратиш, фойдаланиш ёки тарқатиш (278⁶-модда)

Амалиётда мазкур жиноятлар кўпроқ банк-кредит ташкилотларида содир этилади.

Демак мазкур турдаги жиноятларга тааллуқли жиҳат – бу компьютер ахборотининг тушунчаси ва унинг эгасини тўғри аниқлаб олишдан иборат.

Компьютер ахборотлари деганда – ***манбасидан ва тақдим этиш шаклидан қатъий назар шахслар, ашёлар, ҳодисалар, ҳолатлар ва жараёнлар тўғрисидаги маълумотлар*** тушунилади [3].

Ҳар қандай ахборот, агар у билан қонунга хилоф равишда муомалада бўлиш ахборот мулкдори, эгаси, ахборотдан фойдаланувчи ва бошқа шахсга зарар етказиши мумкин бўлса, муҳофаза этилмоғи керак.

Ахборотни муҳофаза этиш:

шахс, жамият ва давлатнинг ахборот соҳасидаги хавфсизлигига таҳдидларнинг олдини олиш;

Ахборотнинг махфийлигини таъминлаш, тарқалиши, ўғирланиши, йўқотилишининг олдини олиш;

Ахборотнинг бузиб талқин этилиши ва сохталаштирилишининг олдини олиш мақсадида амалга оширилади [4].

Ахборот технологиялари соҳасининг ривожланиши янги ижтимоий муносабатларнинг – компьютер муносабатларининг вужудга келиши билан бирга, унга тегишли объектларни жиноят-ҳуқуқий жиҳатдан қўриқлаш муаммосини юзага келтирди.

Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг 20.12.2022 йил кундаги Олий Мажлис ва Ўзбекистон халқига мурожаатномасида Ўқувчиларда эркин ва креатив фикрлашни, жамоада ишлаш ва мулоқот кўникмаларини шакллантириш зарур.

Мана, мактабларимизга қандай муҳит кириб келиши керак!



Бу борада Президент мактабларида 130 та мамлакатда маъқулланган “A-level” таълим дастури йўлга қўйилгани ўз самарасини бермоқда.

Бу жараёнда ҳар бир ўқувчи ўзининг қобилиятига қараб, аниқ йўналишлар бўйича чуқур ўқитилади, дунёнинг нуфузли олийгоҳларига кириш имкониятлари кенгайди.

Шу боис, 2023 йилдан мактаб таълимини халқаро таълим дастурлари асосида бутунлай ислоҳ қилишни бошлаймиз.

Болаларимиз мактабдан она тили ва чет тилларини пухта ўзлаштириб, компьютерда ишлашни ўрганиб чиқиши зарур. Фарзандларимизни касб-хунарларга, санъат ва маданиятга қизиқтиришимиз лозим [5].

Ахборот технологиялари соҳасидаги жиноятларга қарши курашишни тизимли амалга ошириш имкониятини яратди. Уларда жиноятларни тўғри квалификация қилиш ва айбдор шахсларни жинойий жавобгарликка тортиш учун принципиал аҳамиятга эга бўлган кўплаб ҳуқуқий ва техникавий терминларга таърифлар берилди [6].

Компьютер технологиялари соҳасида жиноятлар содир этишга оид статистик маълумотлар шуни кўрсатмоқдаки, уларнинг сони барча ривожланган мамлакатларда йилдан-йилга ўсиб бормоқда. Фақат Россия Федерациясида 2006 йилдан 2016 йилгача ушбу соҳадаги жиноятларнинг сони 300 маротабага ортган. Мамлакатимизда ҳам мазкур жиноятларнинг ортишини башорат қилиш мумкин. Негаки бугунги кунда банк-кредит соҳасидаги, молия-бухгалтерия фаолиятидаги ва бошқа соҳадаги муносабатлар компьютер-ахборот технологияларига асосланади.

Жабрланувчилар камдан-кам ҳолларда ҳуқуқни муҳофаза қилувчи органларга мурожаат этадилар. Компьютер тармоқларидан фойдаланувчиларнинг тўртдан икки қисми ўзларига нисбатан содир этилган жиноятлар ҳақида тегишли идораларга мурожаат қилишни истамасликларини маълум қилганлар.

Ўтказилган ижтимоий сўровлар натижасида аниқланишича, аҳолининг 21% компьютердан уздабуронлик билан фойдаланувчилар ҳисобланади, 28% – ўртамиёна фойдаланувчилар, 51% аҳоли – компьютер билимига эга бўлмаган шахслардир.

Ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятларнинг виктимологик тавсифида ахборот-коммуникация маконида ҳуқуқбузарнинг ҳаракатидан жабрланган шахсларнинг шаклланишида қуйидаги омиллар таъсир кўрсатади деган фикрлар илгари сурилган:

1) *шахснинг туғма психологик хусусиятлари, инсоннинг ғайриқонуний ҳаракатларни амалга оширишга ундайдиган психологик жиҳатлари*. Бунда ёши ва ахборот-коммуникация технологияларидан фойдаланиш қобилиятига кўра қуйидаги шахсларнинг турлари фарқланади:

«**Тажрибасиз**» шахслар ахборот технологиясини яхши билмаган шахслар ҳуқуқбузарликлардан жабрланиш ҳолатлари турли ахборот технологияларида (шахсий компьютер, ноутбук) шахсий истеъмол мақсадларида, яъни мусиқа ўйин ёки турли иловалар тортишда ва компьютердан фойдаланишда ҳамда ҳар хил ўйинларни ўйнашда жабрланади. Улар 15-25-ёшдаги ўсмир ва ёшлар ҳисобланади кўпчилиги эркаклар, ўрта, ўрта махсус ёки олий маълумотли шахслардир [7].

«**Хаваскор**» шахслар компьютер тармоқларида вақти-вақти билан фойдаланадиган, кўп ҳолатларда – техник ходимлар (маъмурлар, техник маслаҳатчилар) бўлиб, эркак



жинсидаги, (кам ҳолатларда аёллар) 20-30 ёшдаги шахслардир. «Ҳаваскор»лар «тажрибасиз» шахс сифатида турли топшириқ ва «буюртмалар»ни бажариш туфайли жабрланадилар.

«Профессионал» шахслар банк ходимлари, бухгалтерия ходимлари, корхона ташкилотда ишловчи техник ходимлар бўлиб компьютер дастурлари ва техник соҳа бўйича барча билим ва кўникмаларга эга, 25-40 ёшдаги шахслар, кўп ҳолатларда эркаклар бўлиб улар пул ва қимматбаҳо қоғозлар операцияларини амалга оширишда жабрланадилар.

2. Ижтимоий хусусиятлар – шахсда хулқ-атвор шаклланишига ижтимоий муҳитнинг таъсири билан боғлиқ омил. Тадқиқот жараёнида ўрганилган шахсларнинг характери ёпиқ, асабий шахсий кечинмалари, уларнинг мактабдаги баҳолари аъло бўлмаган, бироқ информатика асослари ва математика фанларини яхши ўзлаштирмаган ва компьютер хавфсизлиги бўйича малака оширмаган шахсий кўрсаткичлардан иборат.

Тадқиқот ишлари натижасига кўра ахборот технологиялари соҳасидаги жиноятлардан юқори виқтимологик мойиллигига эга жисмоний шахсларнинг ёш ва жинс сифатларига оид типлар ажратилади, булар:

- 21-30 ёшдаги эркаклар (37,2%)
- 31-40 ёшдаги эркаклар (18,5%)
- 21-30 ёшдаги аёллар (12,3%)

Биринчи типдаги жабрланувчилар ҳам эркак, ҳам аёл бўлиши мумкин, уларнинг билим ва маданий даражаси нисбатан юқори (асосан олий техник маълумотга эга) [8].

Шунингдек ахборот технологияларидан фойдаланган ҳолда содир этиладиган жиноятларнинг виқтимологик профилактика фаолиятини ташкил қилиш ва такомиллаштириш мамлакатимизни жадал ривожлантириш ҳамда фуқароларни кибержиноятлар, кибертерроризмдан ва бошқа маънавий таҳдидлардан ҳимоя қилиш, соғлом турмуш тарзини такомиллаштиришга қаратилган чора-тадбирларнинг ажралмас таркибий қисми ҳисобланади.

Ҳозирча киберхавфсизлик Амалий жиҳатдан амалий нуқтаи назардан, ҳар хил вазиятларда ҳар хил одамлар учун мутлақо бошқача маъноларни англатадиган ва ҳар хил тегишли сиёсат, процедуралар ва амалиётларга олиб борадиган оддий атама каби кўриниши мумкин. Ўзининг ижтимоий тармоқларидаги аккаунтларини хакерлик ҳужумларидан ҳимоя қилишни истаган киши, масалан, Пентагон ишчилари томонидан махфий тармоқларни ҳимоялаш учун фойдаланадиган киберхавфсизлик ёндашувлари ва технологияларидан фойдаланиши эҳтимолдан йироқ.

Одатда, киберхавфсизлик қуйидагиларни англатади:

- **шахслар** учун, киберхавфсизлик уларнинг шахсий маълумотлари ўзи ва ўзлари шундай ваколатга эга бўлганлардан бошқа ҳеч ким учун мавжуд эмаслигини ва уларнинг компьютерлари тўғри ишлашини ва зарарли дастурлардан холи эканлигини англатади.
- **кичик бизнес эгалари** учун, киберхавфсизлик кредит карта маълумотлари тўғри ҳимояланганлигини ва маълумотлар хавфсизлиги стандартлари савдо нуқталари регистрларида тўғри бажарилишини таъминлашни ўз ичига олиши мумкин.



- **онлайн бизнес олиб борадиган фирмалар** учун, *киберхавфсизлик* ўз ичига ишончли серверлар билан доимий ишлайдиган серверларни ҳимоя қилиш киради.
- **биргаликда хизмат кўрсатувчи провайдерлар учун**, *киберхавфсизлик* бу ўз навбатида кўплаб турли ташкилотларга тегишли бўлган кўплаб виртуал серверларга эга бўлган кўп сонли серверларни ўз ичига олган кўплаб маълумот марказларини ҳимоя қилишни талаб қилиши мумкин.
- **ҳукумат** учун, *киберхавфсизлик* турли хил таснифлашни белгилашни ўз ичига олиши мумкин, уларнинг ҳар бири ўзига тегишли қонунлар, сиёсат, процедуралар ва технологиялар мавжуд.

Пастки чизиқ шундан иборатки, киберхавфсизлик сўзини аниқлаш осон бўлса-да, одамларнинг онгига ушбу сўзни эшитиш орқали кирадиган амалий умидлар бир оз фарқ қилади.

Пастки чизиқ шундан иборатки, киберхавфсизлик сўзини аниқлаш осон бўлса-да, одамларнинг онгига ушбу сўзни эшитиш орқали кирадиган амалий умидлар бир оз фарқ қилади.

Техник жиҳатдан айтганда, киберхавфсизлик – бу маълумотларнинг электрон шаклда сақланадиган ва ишлов бериладиган ахборот ва ахборот тизимларига мурожаат қиладиган ахборот хавфсизлиги тўплами. *Ахборот хавфсизлиги* маълумотларнинг барча шакллариининг хавфсизлигини ўз ичига олади (масалан, қоғозли файл ва кабинетни таъминлаш).

Бу бугунги кунда кўп одамлар атамаларни сўзма-сўз алмашмоқдалар, кўпинча киберхавфсизликка техник жиҳатдан кирмайдиган, ахборот хавфсизлигининг аспекти сифатида мурожаат қиладилар. Бундай фойдаланиш кўп ҳолатларда иккаласининг аралашishi натижасида юзага келади.

Техник жиҳатдан айтганда, масалан, агар кимдир паролни қоғозга ёзиб қўйса ва қоғозни иш столига ташласа, бошқа одамлар паролни кўришлари мумкин, бу эрда қоғозни депозит қутисига ёки сейфга қўйишнинг ўрнига, у принципни бузган. Киберхавфсизлик эмас, балки ахборот хавфсизлиги, гарчи унинг хатти-ҳаракатлари жиддий киберхавфсизлик оқибатларига олиб келиши мумкин.

Киберхавфсизлик инсон нуқтаи назаридан нимани англатади.

Киберхавфсизлик билан боғлиқ бўлган хатарларни, шунингдек, инсон тажрибасини яхшироқ акс эттирадиган нуқтаи назардан ўйлаш мумкин:

- **Махфийлик хавфи:** Шахсий ёки бошқа махфий маълумотларнинг етарли даражада бошқарилишини ёки суиистеъмол қилинишидан келиб чиқадиган хатарлар.
- **Молиявий хатарлар:** Ҳаск билан боғлиқ молиявий йўқотиш хавфи. Молиявий йўқотишлар тўғридан-тўғри бўлганларни ҳам ўз ичига олиши мумкин – масалан, кимдирнинг банкдаги ҳисоб рақамидан пулни ўғирлаш ҳакер томонидан – ва билвосита зарарлар, масалан, кичик бизнестан кейин ишини йўқотган мижозларнинг йўқолиши. иккинчиси хавфсизлик қоидаларини бузади.
- **Профессинал хавфлар:** Касбий мартаба бузилишидан келиб чиқадиган хатарлар. Шубҳасиз, агар киберхавфсизлик соҳасидаги мутахассислар, агар бузилиш уларнинг назорати остида бўлса ва эҳтиётсизлик туфайли рўй берган бўлса, мансабга зарар етказиш хавфи мавжуд, аммо бошқа турдаги мутахассислар ҳам бузилиш туфайли



мансабга зарар етказиши мумкин. С даражали раҳбарларни ишдан бўшатиш, Кенгаш аъзоларини судга бериш мумкин ва ҳоказо. Хакерлар кимгадир ёмон носозликни кўрсатадиган шахсий алоқа маълумотларини ёки маълумотларини тарқатиб юборишса, масалан, одам бирон бир ноўрин хатти-ҳаракат учун жазоланганлиги, номақбул материалларни ўз ичига олган электрон почта хабарини юборганлиги ва ҳоказо.

- **Бизнес хатарлари:** Бирор шахс учун профессионал хавф-хатарларга ўхшаш бизнес учун хавф. Sony Picturesнинг бузилиши натижасида юзага келган ички ҳужжатлар турли фирмаларнинг компенсация қилиш амалиётига нисбатан салбий нурда бўлган.

- **Шахсий хавфлар:** Кўп одамлар шахсий маълумотларини электрон қурилмаларида, аниқ фотосуратлардан тортиб, ўзларининг ижтимоий доиралари аъзолари томонидан ҳурматга сазовор деб ҳисобланмайдиган тадбирларда қатнашиш тўғрисидаги ёзувларгача сақлашади. Бундай маълумотлар баъзан шахсий муносабатларга жиддий зарар етказиши мумкин. Шунингдек, ўғирланган шахсий маълумотлар жиноятчиларга одамларнинг шахсий маълумотларини ўғирлашда ёрдам беради, бу эса ҳар хил шахсий муаммоларни келтириб чиқариши мумкин.

Охир оқибат, киберхавфсизлик сиз фаолият кўрсатаётган соҳага ва дуч келаётган муаммоларга қараб турли хил таъсирга эга бўлади [9].

Кибержиноят — [компьютер](#) ва [тармоқнинг](#) биргаликдаги алоқаси остида содир этилувчи жиноят тури. Компьютер жиноят пайтида мақсадли йўналтирилган қурол вазифасини бажариб беради. Кибержиноят кимнингдир хавфсизлиги ва молиявий савиясига зарар етказиши мақсадида содир этилади. Анъанавий жиноятчиликнинг камайиши билан глобал ҳамжамиятлар кибержиноятларнинг мунтазам ўсишига гувоҳ бўлишда давом этмоқда. Кибержиноят молиявий жиноятлардан тортиб фирибгарликгача, киберпорнографик савдо ва реклама фирибгарликлари орқали кенг кўламли фаолиятни ўз ичига олади.

Кибертеррорчилик бу таҳдид ёки қўрқитиш орқали, интернетдан фойдаланган ҳолда, сиёсий ёки мафкуравий муваффақиятга эришиш мақсадида уюштирилувчи [кибер ҳужумлардир](#).

[Компьютер вируслари](#), [компьютер қўртлари](#), [фишинг](#), [зарарли дастурлар](#), аппарат усуллари, дастурлаш скриптлари каби воситалар ёрдамида [компьютер тармоқларини](#), хусусан, Интернетга уланган шахсий компьютерларни қасддан, кенг миқёсда бузиш ҳаракатлари интернет терроризмининг кўриниши бўлиши мумкин. Кибертерроризм мунозарали атамадир. Баъзи муаллифлар маълум террористик ташкилотлар томонидан сигнализация, ваҳима ёки жисмоний бузилишларни яратиш мақсадида ахборот тизимларига қарши ҳужумларни бузиш билан боғлиқ жуда тор таърифни танлайдилар. Бошқа муаллифлар эса [кибержиноятни](#) ўз ичига олган кенгроқ таърифни афзал кўришади. Киберҳужумда иштирок этиш, ҳатто зўравонлик билан амалга оширилмаган бўлса ҳам, террор таҳдиди идрокига таъсир қилади. Баъзи таърифларга кўра, онлайн фаолиятнинг қайси ҳолатлари кибертерроризм ёки кибержиноят эканлигини фарқлаш қийин бўлиши мумкин [10].



АОКАда Ички ишлар вазирлиги Киберхавфсизлик маркази масъул ходимлари иштирокида ўтказилган матбуот анжуманида маълум қилинишича, сўнгги 3 йилда мамлакатимизда кибержиноятлар сони бир неча баробарга [ошиб кетган](#).

Таъкидланишича, Ўзбекистонда 25 миллион нафардан ортиқ интернет фойдаланувчилари мавжуд. Ўтказилган таҳлил натижалари эса бугунги кунда мамлакатимизда кибержиноятчиликни ўсиш тенденцияси кузатилаётганлигидан далолат беради. Бугунги кунда энг оммалашган кибержиноятлар эса қуйидагича:

Фирибгарлар пластик карта фойдаланувчиларига келган SMS-хабарномадаги кодларни тўловни амалга ошириш, ютуқни бериш каби баҳоналар орқали эгаллаб, ундаги маблағларни ўзлаштириш;

Шахсий маълумотларни эгаллаш ва уларни ошкор қилиш билан қўрқитиб товламачилик қилиш (кибертовламачилик);

Ижтимоий тармоқда зўрлик ишлатиш билан қўрқитиш, ҳақорат, суусид ҳолатлари (кибербуллинг) ва бошқалар.

Хорижий давлатлар (Туркия, Жанубий Корея, Бирлашган Араб Амирликлари) тажрибасига кўра, интернетдаги таҳдидларга қарши курашишдаги энг самарали усули – бу аҳолида интернетдан фойдаланиш маданиятини шакллантириш орқали уларни эҳтимолий хавфлардан барвақт огоҳлантириш бўлиб, шу мақсадда Ички ишлар томонидан фуқаролар ўртасида фаол тарғиботлар ўтказилган ва бундай тадбирлар билан аҳолини янада кенгроқ қамраб олиш учун мақсадида ИИБ Киберхавфсизлик маркази томонидан “Кибер-ёрдамчи” платформаси ҳам ишлаб чиқилган [11].

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 етказди ва етказилган зарар учун ҳам жавобгар бўлади[12].

References:

1. Ўзбекистон Республикаси ИИВнинг Постда газетасининг 2020 йил 31 декабдаги 48-сон., Б-12.
2. Ўзбекистон Республикаси Президенти Ш.М.Мирзиёевнинг Олий Мажлиснинг Сенати ва Қонунчилик палатасига навбатдаги Мурожаатномаси. 24.01.2020.
3. Ўзбекистон Республикасининг 2003 йилдаги “Ахборот эркинлигининг принциплари ва кафолатлари” тўғрисидаги қонуни 3-модда.
4. Ўзбекистон Республикасининг 2003 йилдаги “Ахборот эркинлигининг принциплари ва кафолатлари” тўғрисидаги қонуни 11-модда.
5. Ўзбекистон Республикаси президенти Шавкат Мирзиёевнинг 20.12.2022 йил кундаги Олий Мажлис ва Ўзбекистон халқига мурожаатномаси.
6. Ўзбекистон Республикасининг “Ахборот эркинлиги принциплари ва кафолатлари тўғрисида”ги 2002 йил 12 декабрь ҳамда “Ахборотлаштириш тўғрисида”ги 2003 йил 11 декабрь қонунлари.
7. Расулев А.К. Ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятларга қарши курашишнинг жиноят-ҳуқуқий ва криминологик чораларини



такомиллаштириш. Юрид. фанлар доктори диссертациясининг автореферати. Т., ИИБ Академияси, 2018. – Б-22.

8. Мухитдинов Ф.М. Жабрланувчи ҳақидаги таълимот асослари / Ўқув-услубий қўлланма., – Т.: ИИБ Академияси, 2019. – Б. 208.

9. <https://uz.bons-sites-web.com/what-is-cybersecurity-16663>

10. <https://uz.wikipedia.org/wiki/kiberjinoyat>

11. <https://www.terabayt.uz/post/ozbekistondagi-kiberjinoyatchilik-holati-haqida-malumot-berdi>

12. Qushboqov S., Yetmishboyev M. Jazoni ijro etish muassasalari ishtirokida tuziladigan fuqarolik-huquqiy shartnomalarning mohiyati va ahamiyati //Eurasian Journal of Law, Finance and Applied Sciences. – 2022. – Т. 2. – №. 9. – С. 76-80.