# КИБЕРМАКОНДА СОДИР БЎЛАЁТГАН ЖИНОЯТЛАРНИНГ СОДИР БЎЛИШ САБАБЛАРИ ВА АХБОРОТ ХАВФСИЗЛИГИГА ТАҲДИДЛАР

**Неъматов Диёрбек Неъматович**

*ИИВ Академияси курсанти*

**Аннотация:** Ушбу мақола кибермаконда содир бўлайотган жиноятларнинг содир бўлиш сабаблари ва ахборот хавфсизлигига таҳдидлар улардан химояланиш бшйича таклиф ва тавфсиялар байон қилинган.

**Аннотация:** В статье описываются причины возникновения преступлений в киберпространстве, а также предлагаются и разъясняются меры защиты от угроз информационной безопасности.

**Abstract** : The article describes the causes of cybercrime and proposes and explains measures to protect against information security threats.

**Калит сўзлар:** Кибержиноят, осон кириш тизими, кичик майдонда маълумотларни сақлаш, далилларни йўқотиш, ахборот хавфсизлиги, таҳдид.

**Ключевые слова:** Киберпреступность, система легкого доступа, хранение данных на небольшой площади, потеря доказательств, информационная безопасность, угроза.

**Key words:** Cybercrime, easy access system, data storage in a small area, loss of evidence, information security, threat.

Кибержиноятнинг асосий таъсири молиявийдир. Кибержиноятлар фойда келтирувчи жиноий фаолиятнинг кўплаб турларини, жумладан, тўловга қарши ҳужумлар, электрон почта ва интернетдаги фирибгарлик, шахсий маълумотларга оид фирибгарликларни, шунингдек, молиявий ҳисоб, кредит карта ёки бошқа тўлов картаси маълумотларини ўг‘ирлашга уринишларни ўз ичига олиши мумкин. Кибержиноятчилар шахснинг шахсий маълумотларини ёки корпоратив

маълумотларини ўғирлаш ва қайта сотиш учун нишонга олишлари мумкин. Пандемия туфайли кўплаб ишчилар масофавий иш тартибига ўтаётганлиги сабабли, 2021-йилда кибержиноятлар тез-тез ўсиши кузатилди, бу эса заҳиравий маълумотларни ҳимоя қилишни аҳамиятини оширди. Интернетга уланиш зарурати кибержиноятчилик фаолиятининг ҳажми ва суръатини оширишга имкон берди, чунки жиноят содир этганда жиноятчи жисмонан ҳозир бўлиши шарт эмас. Интернет тезлиги, қулайлиги, анонимлиги ва чэгараларнинг йўқлиги компютерга асосланган молиявий жиноятларни - тўлов дастури, фирибгарлик ва пул ювиш, шунингдек, таъқиб қилиш ва безорилик каби жиноятларни амалга оширишни осонлаштиради. Кибержиноятчилик фаолияти нисбатан кам техник малакага эга бўлган шахслар ёки гуруҳлар ёки юқори даражада уюшган глобал жиноий гуруҳлар томонидан амалга оширилиши мумкин, улар орасида малакали ишлаб чиқувчилар ва тегишли тажрибага эга бўлган бошқалар ҳам бўлиши мумкин. Аниқлаш ва жиноий жавобгарликка тортиш имкониятларини янада камайтириш учун кибержиноятчилар кўпинча кибержиноят қонунлари заиф ёки мавжуд бўлмаган мамлакатларда фаолият юритишни афзал кўрадилар. Интернетдан ташқарида содир этилган кўплаб жиноятларда бўлгани каби, пул кўплаб кибер жиноятчилар учун асосий туртки ҳисобланади. Айниқса, сиз тармоқ орқасида яширинганингизда жиноятчилик хавфи унчалик сезилмаганлиги сабабли паст хавф ва жуда юқори молиявий мукофотни идрок этиш кўплаб кибер жиноятчиларни зарарли дастурлар, фишинг, шахсий маълумотларни ўғирлаш ва фирибгар пул сўрови ҳужумларида қатнашишга ундайди.

Жиноятчиларни рағбатлантирадиган сабаблардан ташқари, кибержиноят содир бўладиган муҳит ҳам бу ҳодисанинг кенг тарқалганлигини тушунтиришга хизмат қилади. Битта муваффақиятли киберҳужумнинг оқибатлари молиявий йўқотишлар, интеллектуал мулкни ўғирлаш ва истеъмолчиларнинг ишончи ва ишончини йўқотиш каби кенг қамровли оқибатларга олиб келиши мумкин. Кибержиноятнинг жамият ва ҳукуматга умумий пул таъсири йилига миллиардлаб долларни ташкил қилади.

Кибержиноятчиларнинг асосий мақсади катта пул топиш ёки махфий маълумотлардан ноқонуний фаолият учун фойдаланишдир. Улар, асосан, бой одамлар ёки банклар, казинолар ва ҳар куни катта миқдордаги пул оқиб тушадиган молиявий фирмалар каби бой ташкилотларни нишонга олади. Бундан ташқари, махфий маълумотларни ўз ичига олган ташкилотлар ҳам нишонга олинади. Кибер жиноятчилар одатда тизимларни бузиб, нозик маълумотларни ўғирлайдилар. Шу ўринда кибержиноятлар содир бўлишининг асосий сабабларини келтириб ўтамиз:

**Осон кириш тизими**

Тизимни мураккаб технологияларни ўз ичига олган маълумотлар бузилишидан ҳимоя қилиш кўпинча қийин ёки имконсиздир. Хавфсизлик фақат хакерлар учун тизимга кириш осон бўлгандагина бузилиши мумкин. Малакали хакерлар кириш кодларини бузиш орқали рухсатсиз кириш ҳуқуқига эга бўлишлари мумкин. Улар биометрик тизимни осонгина алдашлари ва тизимнинг хавфсизлик девори орқали ўтишлари мумкин.

**Кичик майдонда маълумотларни сақлаш**

Маълумки, компютер жуда катта ҳажмдаги маълумотларни ихчам жойда сақлайди ва бу киберҳужумлар ортидаги энг катта сабаблардан биридир. Айнан компютерлар кашф этилгандан кейин кибержиноят пайдо бўлди. Кичкина жойда маълумотларни сақлаш хакерларга қисқа вақт ичида маълумотларни ўғирлаш ва улардан ўз фойдалари учун фойдаланишни осонлаштиради. Шунинг учун тизимда барча керакли маълумотларни сақламаслик ва уларни турли жойларда ажратиш тавсия этилмоқда.

**Мураккаб кодлашлар**

Операцион тизимлар компютерларни функсионал қилади ва бу операцион тизимлар миллионлаб кодлар билан яратилган. Операцион тизимлар инсонлар бўлган ишлаб чиқувчилар томонидан дастурлаштирилган ва шу билан кодларни хатоларга қарши ҳимоясиз қилди. Кодлардаги энг кичик ҳалқа операцион тизим функсияларида катта фарқ қилмаслиги мумкин бўлса-да, бу бўшлиқлардан кибер-жиноятчи осонликча

фойдаланиши мумкин. Улар ушбу бўшлиқлардан ўтиб, операцион тизимни фойдаланувчилар учун зарарли қилишлари мумкин. Мураккаб кодлаш кўпинча кибер жиноятларнинг умумий сабабига айланиши мумкин.

**Бепарволик**

Биз эътиборсиз қолдирадиган ва эътиборсиз қолдириш осон деб ҳисоблаган ҳар қандай нарса жиддий ташвишга айланиши мумкин. Кибержиноят худди шундай ишлайди. Тизимингиз хавфсизлигини таъминлашда бепарволик сизга катта муаммоларни келтириб чиқариши мумкин. Сизнинг охирида бироз бепарволик кибержиноятчилар учун меҳмондўст йўлак бўлиши мумкин. Шунинг учун тизимингиздаги воқеаларга ҳушёр бўлишингиз керак.

**Далилларни йўқотиш**

Хакерлар одатда тизимингизга бўлимларга бўлинган ҳолда ҳужум қилишади ва уларнинг биринчи бузилиши ҳақидаги далилларни осонгина йўқ қилиш мумкин. Бу уларнинг жиноятларини янада кучлироқ қилади, бу эса кибержиноятларни тергов қилиш жараёнида аниқланмайди. Далилларнинг йўқолиши кибержиноятнинг муҳим сабабига айланиши мумкин, бу сизнинг тизимингизни фалаж қилиши ва уни киберҳужумларга нисбатан заифроқ қилиши мумкин.

**Заиф амалга ошириш қонуни**

Кибержиноятлар нисбати кундан кунга ортиб бормоқда. Амалга оширишнинг заиф қонуни кибержиноятларнинг сабабларидан биридир, чунки айбдорлар бир неча кундан кейин ўзларини озод қилишлари мумкинлигини билишади ёки улар ўзларининг жиноятларига нисбатан минимал даражага ега бўлишади, чунки кибержиноятлар учун қатъий ва тезкор қоидалар йўқ. Бу кўпроқ кибержиноятларга олиб келади. Одатда фойдаланувчилар эсда сақлаш осон бўлган пароллардан фойдаланишга ҳаракат қиладилар. Бироқ, бундай йўл тутиш бузғунчи учун паролларни тахминлаб топиш имкониятини оширади. Бошқа томондан, мураккаб пароллардан фойдаланиш ва уларни турли элтувчиларда сақлаш (масалан, қоғозда

қайд этиш) эса, ушбу муаммони янада кучайтиради. Бу мисоллар инсон омили туфайли турли жойлар ва ҳолатларда хавфсизлик муаммоларининг келиб чиқиши мумкинлигини кўрсатади. Инсон омили туфайли юзага келадиган хавфсизлик муаммоларига кўплаб мисоллар келтириш мумкин. Бироқ, келтирилган ҳолатлардаги энг муҳим жиҳат шундаки, хавфсизлик нуқтаи назаридан “тенгламадан” инсон омилини олиб ташлаш зарур. Бошқача айтганда, инсон омили иштирок этмаган тизимлар иштирок этган тизимларга нисбатан хавфсизроқ бўлади.

**Энг муҳим инсон омилларига қуйидагилар тааллуқли:**

—Киберхавфсизлик соҳасига оид билимларни етишмаслиги катта ҳажмдаги ошкор заифликларни пайдо бўлишига олиб келади. Киберхавфсизлик соҳаси анъанавий хавфсизликка алоқадор бўлгани боис, зарур технологик мослашишнинг тезкорлиги кўп ҳолларда бўлиши мумкин бўлган заифликлар сонини оширади. Бошқа томондан, инсоннинг соҳага тегишли сўнгги технологик билимларни ўзлаштириши ҳар доим ҳам етарли бўлмайди.

—Рискларни бартараф этишни ва улар ҳақида хабар беришнинг етарли бўлмаслиги киберхавфсизликда такрорланувчи ва кутилмаган бузилишларга сабабчи бўлади. Инсонлар одатда ташкилотларига жиддий хавф солувчи риск мавжудлигини билишсада, уни ошкор қилишмайди. Бунинг асосий сабаби сифатида риск бевосита шахснинг ўзига, уни молиявий ҳолатига таъсир этмаслигини ёки ошкор қилинганида шахснинг обрўси тушишини келтиришади.

—Маданият ва муносабатлардаги муаммоларга ташкилотнинг ўзи ёки ташкилот ички маълумотларини билувчи норози ва эътиборсиз ходимнинг пайдо бўлиши сабабчи бўлиши мумкин. Киберхавфсизлик муаммоларининг аксарияти ички ҳисобланиб, улар ходимлар орасидаги турли келишмовчиликлар ва ташкилот ичидаги муҳитнинг яхши эмаслиги натижасида юзага келади. Бу сабаблар эса, ходимнинг ташкилот ички структурасини яхши билгани боис, аксарият ҳолларда жиддий муаммоларга олиб келади.

—Хавфсизлик машғулотларига кам маблағ сарфланиши бошқарилаётган хавфсизлик рисклари тўғрисидаги маълумотнинг камлиги сабабчи бўлади. Одатда, соҳа корхоналаридаги ходимлар мустақил равишда киберхавфсизлик қоидаларини ўрганишмайди. Шунинг учун киберхавфсизлик қоидаларини ходимларга махсус машғулотлар шаклида етказиш зарур бўлади. Бу эса ташкилотдан хавфсизлик машғулотларига етарлича маблағ сарфланишни талаб қилади.

—Ҳисобга олиш нуқтасининг ягона эмаслиги натижасида хавфсизликнинг тўлақонли амалга оширилмаслиги кузатилади. Амалда хавфсизликни кафолатли таъминлашда унинг назоратини бир нуқтада амалга ошириш муҳим ҳисобланади. Ягона нуқтада амалга оширилган хавфсизлик назорати тақсимланган шаклига нисбатан ишончли бўлади. Бироқ, ташкилотлардаги хавфсизлик назоратининг мураккаблиги боис, назорат одатда тақсимланган ҳолда бошқарилади.

—Ижтимоий инжинерия асосида хавфсизлик назоратини айланиб ўтишда фойдаланувчидан, анъанавий жосуслик техникаси ёрдамида, маълумотлар қўлга киритилади. Энг яхши киберхавфсизлик тизимига эга бўлган ташкилотга ҳам ижтимоий инжинерия таҳдиди хавф солиши мумкин. Айниқса, фойдаланувчиларни турли ижтимоий тармоқларда шахсий маълумотларини эътиборсизлик билан қолдириши бу хавфнинг кескин ортишига сабабчи бўлмоқда.

**Кибержиноят амалга оширилганида қуйидагилар асосий мақсад сифатида қаралади:**

—маблағ, қимматли қоғозлар, кредит, моддий бойликлар, товарлар, хизматлар, имтиёзлар, кўчмас мулк, ёқилғи хом ашёси, энергия манбалари ва стратегик хом ашёларни ноқонуний ўзлаштириш;

—солиқ ва бошқа йиғимларни тўлашдан бош тортиш; - жиноий даромадларни қонунлаштириш;

—қалбаки ҳужжатлар, штамплар, муҳрлар, бланкалар, шахсий ютуқ чипталарини қалбакилаштириш;

—шахсий ёки сиёсий мақсадларда махфий маълумотларни олиш;

—маъмуриятнинг ёки ишдаги ҳамкасбларнинг ғаразли муносабатлари учун қасос олиш;

—шахсий ёки сиёсий мақсадлар учун мамлакат пул тизимини бузиш;

—мамлакатдаги вазиятни, ҳудудий маъмурий тузилишни беқарорлаштириш;

—талончилик, рақибни йўқ қилиш ёки сиёсий мақсадлар учун муассаса, корхона ёки тизим иш тартибини бузиш;

—шахсий интелектуал қобилиятини ёки устунлигини намойиш қилиш.

**Кибержиноят турларини қатъий таснифлашнинг имкони йўқ. Қуйида криминология соҳасига нисбатан кибержиноятларнинг турлари келтирилган:**

- иқтисодий компютер жиноятчилиги;
- инсон ва фуқароларнинг конституциявий ҳуқуқлари ва эркинликларига қарши қаратилган компютер жиноятчилиги;
- жамоат ва давлат хавфсизлигига қарши компютер жиноятчилиги. Иқтисодий компютер жиноятчилиги амалда кўп учрайди. Улар жиноятчиларга миллионлаб АҚШ доллари миқдоридаги ноқонуний даромадлар келтиради. Улар орасида кенг тарқалгани фирибгарлик, асосан, банк ҳисоб рақамлари ва банк карталари орқали амалга оширилади. Халқаро амалиётда пластик карталар билан содир этилган жиноятлар йўқолган ёки ўғирланган карталар, сохта тўлов карталарини яратиш ёки улардан фойдаланиш, карта тақдим этмасдан банк ҳисоб варағи маълумотларини олиш ва ноқонуний фойдаланиш, шунингдек, карта эгаси томонидан содир этилган жиноятлар билан боғлиқ.

Юқоридаги ҳолатларни камайтириш ахборотни таҳдидлардан қанчалик даражада муҳофаза килинганлик даражасига боғлиқ. Ахборотни самарали ҳимоя қилишни таъминлаш учун биринчи навбатда ахборот хавфсизлигига таҳдид соладиган барча омилларни ҳисобга олиш ва таҳлил қилиш зарур. Ахборот хавфсизлигига таҳдид

одатда тизимга ва унда сақланадиган ва қайта ишланадиган маълумотларга кирувчи таъсир кўрсатиши мумкин бўлган потенциал ҳодиса, ҳаракат, жараён ёки ҳодиса сифатида тушунилади. СОП таркибий қисмлари орқали ахборотга таъсир қилувчи бундай таҳдидлар ахборотни йўқ қилиш, бузиш, нусхалаш, рухсациз тарқатиш, унга киришни чеклаш ёки блокировка қилишга олиб келиши мумкин. Ҳозирги вақтда таҳдидларнинг жуда кенг рўйхати маълум бўлиб, улар бир нечта мезонларга кўра таснифланади.

**Фойдаланилган адабиётлар рўйхати:**

**I. Ўзбекистон республикаси конституцияси, қонунлари ва кодекслари:**

1. Ўзбекистон Республикасининг Конституцияси, 08.12.1992 й.;
2. Ўзбекистон Республикасининг Жиноят кодекси, 22.09.1994 й.;
3. Ўзбекистон Республикасининг Маъмурий жавобгарлик тўғрисидаги кодекси 22.09.1994 й.;
4. Ўзбекистон Республикасининг ЗРУ137сонли “Ахборотлаштириш ва маълумотлар узатиш соҳасида қонунга хилоф ҳаракатлар содир этганлик учун жавобгарлик кучайтирилганлиги муносабати билан Ўзбекистон Респуб ликасининг айрим қонун ҳужжатларига ўзгартиш ва қўшимчалар киритиш тўғрисида»ги Қонуни, 25.12.2007 й.;
5. Ўзбекистон Республикасининг 560IIсонли “Ахборотлаштириш тўғрисида»ги Қонуни, 11.12.2003 й.;
6. Ўзбекистон Республикасининг ЗРУ547сонли “Шахсий маълумотлар тўғри сида»ги Қонуни, 02.07.2019 й.;
7. Ўзбекистон Республикасининг 439IIсонли “Ахборот эркинлиги принцип лари ва кафолатлари тўғрисида»ги Қонуни, 12.12.2002 й.;
8. Ўзбекистон Республикасининг ЗРУ395сонли “Электрон ҳукумат тўғрисида»ги Қонуни, 09.12.2015 й.;