



КИБЕРЖИНОЯТЛАР, УЛАРНИНГ ЖАМИЯТ ОРАСИДА КЕНГ ТАРҚАЛГАН ТУРЛАРИ ВА УЛАРГА ҚАРШИ КУРАШИШНИНГ ЎЗИГА ХОС ЖИХАТЛАРИ

Ашуров Отабек Умматиллаевич

Ўзбекистон Республикаси ИИБ Академияси
Тезкор қидирув фаолияти кафедраси ўқитувчиси

Усмонов Асадбек Исроил ўғли

ИИБ Академияси курсанти

<https://doi.org/10.5281/zenodo.11195607>

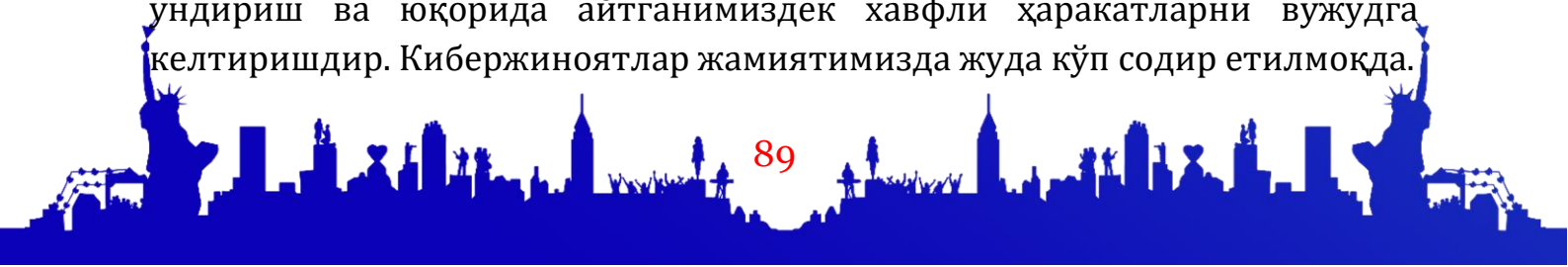
Аннотация: Мазкур мақолада интернет тармоғи ва ахборот технологиялари соҳасида юз бераётган кибержиноятлар ҳақида қисқача ёритилган. Шунингдек, ушбу жиноятларнинг турлари, бу турдаги жиноий вазиятларга қарши кураш тизимини такомиллаштириш, хавфсизлик чораларини кўриш бўйича қонунчилигимизда самарали олиб борилаётган ислохотлар ёритилган.

Калит сўзлар: киберхавфсизлик, кибержиноят, фишинг, вишинг, смишинг, фарминг, скимминг, спам.

Сўнгги пайтларда ижтимоий тармоқларда сайтларни бузиб кириш, вирусли дастурлар тарқатиш каби ҳолатлар жуда кўп учрамоқда. Кибер жиноятлар ҳозирги глобаллашув даврида жиддий муаммолардан бирига айланди. Кибержиноятчилик атамаси компьютерлар, тармоқлар ёки интернетни қамраб олувчи жиноий фаолиятни назарда тутди. Кибержиноятларга қарши курашиш учун ИТ-компаниялар ҳар доим инсон омилини ҳисобга олишлари керак, чунки ҳозирги вақтда тажовузкорлар ижтимоий муҳандислик усулларида фаол фойдаланади. Кибержиноятлар асосан молиявий даромад олиш мақсадида амалга оширилади. Янги технологиялар замонида янгича атамалар билан ҳам таниш бўлишимиз зарур. Улардан бири "Киберхавфсизлик".

Киберхавфсизлик - кибермаконда шахс, жамият ва давлат манфаатларининг ташқи ва ички таҳдидлардан ҳимояланганлик ҳолати. Кўриниб турганидек, киберхавфсизлик бузиладиган бўлса, шахс, жамият, давлат манфаатлари поймол етиларкан. Бундай киберхавфсизликка қарши ҳар қандай хавфли ҳаракатларни кибержиноят дейиш мумкин.

Кибержиноят — компьютер ва тармоқнинг биргаликдаги алоқаси остида содир этилувчи жиноят тури. Давлатга, жамиятга хавф туғдирадиган ҳаракатларни пайдо қилади. Бунда асосий мақсад пул ундириш ва юқорида айтганимиздек хавфли ҳаракатларни вужудга келтиришдир. Кибержиноятлар жамиятимизда жуда кўп содир етилмоқда.





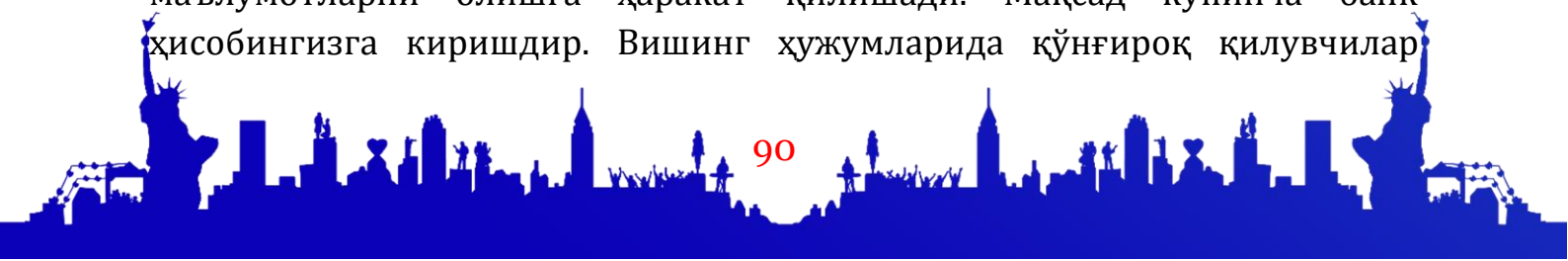
Тўлов карталари билан фирибгарлик, кардинг (инглизча – “сардинг”) - бу фирибгарлик тури бўлиб, унда тўлов картаси ёки унинг реквизитлари ёрдамида унинг эгаси томонидан бошланмаган ёки тасдиқланмаган операция амалга оширилади. Тўлов картаси маълумотлари одатда онлайн-дўконларнинг бузилган серверларидан, тўлов ва ҳисоб-китоб тизимларидан, шунингдек шахсий компьютерлардан (тўғридан-тўғри ёки масофавий кириш дастурлари орқали, “троянлар”, “шаклларни тортиб олиш” функцияси билан “ботлар”) олинади. Тўлов карталари бўйича фирибгарлик соҳасидаги енг йирик жиноятлардан бири Ворлдпай глобал кредит карта процессорига бузиб кириш ва унинг маълумотларидан фойдаланган ҳолда 9 миллион доллардан ортиқ маблағни ўғирлаш ҳисобланади. 2009-йил ноябрь ойида ушбу иш бўйича МДХ давлатлари фуқароларидан иборат жиноий гуруҳга қарши айбловлар қўйилган.

Бундан ташқари, бугунги кунда тўлов карталари рақамларини ўғирлашнинг енг кенг тарқалган усули бу фишинг (инглизча - фишинг, бузилган “балиқ овлаш” - “балиқ овлаш”) - фирибгарлар томонидан фойдаланувчи томонидан ишончли бўлган сайтни яратишдир.

Фишинг – бу кибержиноят бўлиб, унда мақсадли электрон почта, телефон ёки матнли хабар орқали қонуний муассаса сифатида намоён бўлган шахс томонидан жисмоний шахсларни шахсий идентификациялаш мумкин бўлган маълумотлар, банк ва кредит карта маълумотлари ва пароллар каби махфий маълумотларни тақдим етишга жалб қилиш учун боғланади.

Фишинг бўйича биринчи ҳужум 2004-йилда “Америса Онлине” веб-сайтига тақлид қилган Калифорниялик ўсмирга қарши қўзғатилган. Ушбу сохта веб-сайт ёрдамида у фойдаланувчилардан махфий маълумотларни олишга ва уларнинг ҳисобларидан пул олиш учун кредит карта маълумотларига киришга муваффақ бўлди. Электрон почта ва веб-сайтдаги фишингдан ташқари, “вишинг” (овозли фишинг), “смишинг” (СМС фишинг), “скимминг” ва кибер жиноятчилар доимий равишда ўйлаб топадиган бошқа бир қанча фишинг усуллари ҳам мавжуд.

Вишинг - бу телефон орқали содир бўладиган ижтимоий муҳандислик ҳужумининг бир тури. Қўнғироқ қилганлар бошқа жиноят содир етишда фойдаланиш учун сизнинг шахсингизни тасдиқловчи маълумотларни олишга ҳаракат қилишади. Мақсад кўпинча банк ҳисобингизга киришдир. Вишинг ҳужумларида қўнғироқ қилувчилар





сизни ўзаро алоқада бўлишга ишонтириш учун ижтимоий меъёрлар ва умидларга таянадилар. Улар ўзларини ҳукумат, полиция, солиқ департаменти ёки банкингизнинг одамлари деб кўрсатишади. Ишончли ҳокимият сизга кўнғироқ қилганда, сиз асабийлашингиз, қизиқувчан бўлишингиз ёки жавоб бериш учун ҳақиқий бурчни ҳис қилишингиз мумкин. Фирибгарлар буни билишади ва сизни жалб қилиш учун бу ҳис-туйғулардан фойдаланадилар. Вишинг жиноятчилар сизни муаммога дуч келганингизга ишонтириш учун телефон орқали таҳдид ва психологик тактикалардан фойдаланадилар.

Смишинг - бу мобил қурилмалардан хужум платформаси сифатида фойдаланадиган фишинг тури. Кредит карта рақамлари ва шахсий маълумотларни олиш учун кибержиноятчи хужумлар. СМС-хабарлар шиддатли хужумни амалга ошириш учун ишлатилади, шунинг учун номи (СМС + фишинг). Смишинг хужумлари матнли хабарларни юбориш учун СМС ёки бошқа хизматлардан фойдаланади. Хужумнинг ушбу шакли одамлар электрон почтадан кўра телефон орқали олинган хабарларга кўпроқ ишонишлари сабабли тобора оммалашиб бормоқда. Кўпчилик фишинг хужумларини СМС билан боғламайди, гарчи аслида тажовузкорлар учун телефон рақамини олиш электрон почта манзилидан кўра осонроқдир.

Фарминг - бу қурбонни ёлғон ИП-манзилга яширин тарзда йўналтириш тартиби. Бунинг учун навигация структурасидан (хост файли, домен номлари тизими (ДНС)) фойдаланиш мумкин. Классик фишингда бузғунчи ижтимоий тармоқлар, онлайн-банкнинг ва веб-почта хизматлари фойдаланувчилари ўртасида электрон почта хабарларини тарқатади, алдаш қурбони бўлган фойдаланувчиларни логин ва паролларини олиш учун сохта сайтларга жалб қилади. Замонавий веб-хизматлардан фаол фойдаланадиган кўплаб фойдаланувчилар фишингнинг ўхшаш ҳолатларига бир неча марта дуч келишган ва шубҳали хабарлардан эҳтиёт бўлишади. Классик фишинг схемасида бутун схеманинг самарадорлигини белгилайдиган асосий "заиф" ҳавола бу фойдаланувчига боғлиқлик - у фишерга ишонадими ёки йўқми. Шу билан бирга, вақт ўтиши билан фойдаланувчиларнинг фишинг хужумлари ҳақида хабардорлиги ошди.

Скимминг (инглизча "то ским" - равон ўқинг, силжитинг) - бу банк карталари билан фирибгарликнинг бир тури бўлиб, махсус техник мослама ёки скиммер ёрдамида уларнинг магнит чизиғидан маълумотларни ўқишни ўз ичига олади. Фирибгарлар жабрланувчининг





ПИН кодини ҳам билишга ҳаракат қилади. Карта маълумотларини олганингиздан сўнг, сиз уни нусхалашингиз ва барча пулларни олишингиз мумкин. Маълумотларни ўқиш учун скиммерлар ишлатилади - тўғридан-тўғри банкоматга, шунингдек картани ўқувчининг ҳар қандай қабул қилиш уясига уланган махсус қурилмалар. Фирибгарлар кўчма магнит чизиқли ўқувчиларни меҳмонхоналар, кафе ва ресторанлар, дўконларга ўрнатиши мумкин.

Спам- бу ёзишмаларни олиш истагини билдирмаган шахсларга оммавий юбориш. Спам тарқатувчилар спамерлар деб аталади. Умумий қабул қилинган маънода рус тилидаги "спам" атамаси биринчи марта электрон почта хабарларини жўнатиш учун ишлатилган. Тезкор хабар алмашиш тизимларида (масалан, ИСҚ) кировчи хабарлар Мессагинг деб аталади.

Кибержиноятларга қарши кураш бир қатор омиллар билан мураккаблашади ва аниқ:

- кибержиноятчилар оддий фирибгарлар емас, балки яхши ўқитилганлардир, компьютер экрани орқасида яширинган дастурчилар, шунга ўхшаш шахсни ҳисоблаш оддий жиноятчига қараганда анча қийин.

- кибержиноятларга дуч келганда, ҳуқуқни муҳофаза қилиш органлари ходимлари, ҳокимият органлари юқори малакали мутахассислар ёрдамига муҳтож етишмовчиликда давом этаётган дастурлаш соҳаси.

- фактнинг ўзини аниқлашда кўп қийинчиликлар пайдо бўлади, ушбу жиноятни содир етиш.

Замонавий дунёда кибержиноят жамият ва унинг ахборот хавфсизлигига жиддий таҳдид солмоқда. Кибержиноят зудлик билан жавоб бериш ва самарали ҳал етишни талаб қилувчи ижтимоий муаммолар мажмуасини келтириб чиқаради. Ахборот технологияларининг такомиллашуви билан кибержиноятчилик ҳам такомиллашиб бормоқда, бу одамлар ва умуман жамият ҳаёти ва фаолиятининг кўплаб соҳаларида ўзини намоён қилади. Ушбу турдаги жиноятлардан ҳимоя қилиш халқаро ҳамкорлик ва ўзаро ҳамкорлик даражасидаги саъй-ҳаракатларнинг ўзаро боғлиқлигини талаб қилади.

Ахборот соҳасидаги ҳуқуқбузарликлар ва кибержиноятларга қарши самарали курашиш сиёсатини амалга ошириш учун қуйидаги чоратadbирларни амалга ошириш лозим:





- тармоқдаги кибержиноятларни аниқлашга ёрдам берувчи технологияларни ва дастурларни, шунингдек, ушбу жиноятларни тергов қилиш усуллари тақомиллаштириш;

- кибер таҳдидларга қарши курашиш учун блокчейн технологиясидан максимал даражада фойдаланиш;

- сунъий интеллект ресурсларини ривожлантириш ва уларни кибержиноятларни тергов қилиш соҳасида изчил жорий этиш;

- кибержиноятларни содир этганлик учун жазо чораларини кучайтириш;

- барча мумкин бўлган шакл ва кўринишларда кибертерроризмга қарши мақсадли курашиш.

Юқорилардагидан хулоса қилиб шуни айтиш мумкинки, ахборот технологиялари соҳаси жадал ривожланиб бораётган замонда у билан боғлиқ турли-туман муаммолар юзага келмоқда. Шундай экан, интернет хавфсизлигини таъминлаш ва бу каби жиноятларнинг олдини олиш фақатгина давлатнинг емас, балки интернет хизматидан фойдаланаётган ҳар бир мустақил шахснинг ҳам бурчи ҳисобланмоғи даркор. Ходимларни киберхавфсизлик асосларига ўргатиш ушбу соҳада харажатларни янада самарали режалаштиришга ёрдам беради.

Адабиётлар:

1. "Киберхавфсизлик тўғрисида"ги қонун. ЎРҚ-764-сон
2. Қаршиев А. Ўрта асрлардаги тезкор-қидирув тадбирларини айрим жиҳатлари //Евразийский журнал права, финансов и прикладных наук. – 2024. – Т. 4. – №. 4. – С. 180-187.
3. Каршиев А.М. К вопросу о понятии «оперативная комбинатсия» //образование наука и инноватсионные идеи в мире. – 2023. – Т. 25. – №. 1. – С. 68-71.
4. Каршиев А.М. и др. Нормативно-правовая регламентация обеспечения компьютерной безопасности информационных систем в республики узбекистан //образование наука и инноватсионные идеи в мире. – 2023. – Т. 25. – №. 1. – С. 77-82.
5. Якубов Х.Ш. Тезкор-қидирув психологиясининг аҳамияти //образование наука и инноватсионные идеи в мире. – 2023. – Т. 25. – №. 2. – С. 38-44.
6. Якубов Х. Ш. Тезкор эксперимент тезкор-қидирув тадбирининг тушунчаси //Лучшие интеллектуальные исследования. – 2023. – Т. 11. – №. 5.

