7 – TOM 6 – SON / 2024 - YIL / 15 - IYUN

КИБЕР МАКОНДА СОДИР ЭТИЛАДИГАН ЖИНОЯТЛАР, ОЛДИНИ ОЛИШДА КИБЕР ХАВФСИЗЛИКНИ ТАЪМИНЛАШНИНГ ЎРНИ

Сафарова Дилбар Бахрилла Кизи
ИИВ академияси курсанти

Аннотатсия: *Ushbu maqolaning долзарблиги кибер маконда содир этиладиган жиноятлар, уларни турлари, олдини олишда кибер хавфсизликни таъминлашнинг ўрнини ўрганишдан иборат. Мазкур maqolaningнинг мақсади ахборот технологияларидан фойдаланиб содир этиладиган жиноятлар турларини, кибержиноятларнинг ривожланиши ва сабабларини, унинг ўзига хос хусусиятларини аниқлаш, кибермакон тушунчаси, унда содир этилиши мумкин бўлган жиноятлар статистикасини ўрганиб чиқиб, сабаб шароитларни аниқлаш, кибержиноятчиликни олдини олиш мақсадида жамоатчиликка кенг тарғиб этиб, келажакда шу каби жиноят қурбонлари ёки ушбу жиноятларни субъекти бўлишини олдини олиш. Замон техника ютуқлардан фойдаланиб, кибержиноятларни фош этиш, илғор хорижий давлатлар тажрибаларини ўрганиб уни амалиётга татбиқ этиш чора тадбирлар юзасидан таклиф ва тавсиялар ишлаб чиқилган.*

Аннотация: *Актуальность данной статьи заключается в изучении преступлений, совершаемых в киберпространстве, их видов, а также роли кибербезопасности в предотвращении. Цель данной статьи - определить виды преступлений, совершаемых с использованием информационных технологий, развитие и причины киберпреступлений, их специфические характеристики, понятие киберпространства, статистику преступлений, которые могут быть совершены в нем, определить причинные условия, широко распространить его среди общественности, чтобы предотвратить киберпреступность и в будущем не допустить, чтобы жертвы таких преступлений или субъекты этих преступлений стали жертвами таких преступлений.*

Abstract: ***The relevance of this article is the study of crimes committed in cyber space, their types, and the role of cyber security in prevention. The purpose of this article is to determine the types of crimes committed using information technologies, the development and causes of cybercrimes, its specific features, the concept of cyberspace, the statistics of crimes that can be committed in it, and to determine the causal conditions, to promote it to the public in order to prevent cybercrime, and in the future to prevent victims of such crimes or becoming subjects of these crimes.***

Киберҳужум - бу компьютер тизимлари, технологияга боғлиқ корхоналар ва тармоқлардан атайлаб эксплуататсия қилиш. Киберҳужумлар компьютер кодини, мантиқини ёки маьлумотларини ўзгартириш учун зарарли коддан фойдаланади, натижада маьлумотларнинг бузилиши ва маьлумотлар ва шахсни ўг‘ирлаш каби

кибержиноятларга олиб келиши мумкин бўлган бузувчи оқибатларга олиб келади. Киберҳужум компьютер тармоғига ҳужум (**CHA**) сифатида ҳам танилган. **Киберҳужумлар қуйидаги оқибатларга олиб келиши мумкин:**

- Шахсни ўғирлаш, фирибгарлик, товламачилик
- Зарарли дастурлар, пҳарминг, фишинг, спам, споофинг, жосуслик дастурлари, троянлар ва вируслар
- Ноутбуклар ёки мобил қурилмалар каби ўғирланган аппарат
- Хизматни рад этиш ва тарқатилган хизматдан бош тортиш ҳужумлари
- Киришнинг бузилиши
- Паролни ҳидлаш
- Тизимнинг инфилтратсияси
- Веб-сайтни бузиш
- Шахсий ва оммавий веб-браузер эксплуататсиялари
- Тезкор хабарларни суиистеъмол қилиш
- Интеллектуал мулк (ИП) ўғирланиши ёки рухсатсиз кириш

Дартмут университети қошидаги Хавфсизлик технологияларини ўрганиш институти ҳуқуқни муҳофаза қилиш органлари текширувлари олдида турган киберҳужум муаммоларини тадқиқ қилади ва текширади ва ИПни кузатиш, маълумотларни таҳлил қилиш, реал вақт режимида ушлаш ва миллий маълумотларни алмашишнинг узлуксиз ривожланишига эътибор қаратади.

Кибер-жиноятнинг умумий мисоллари қуйидагилардир:

1. Malware (Зарарли дастур)
2. Phishing (Балиқ овлаш)
3. Password attacks (Парол ҳужими)
4. DDOS attacks (ДДОС ҳужими)
5. Man in the Middle (Оъртадаги одам)
6. Drive-by download (Машинада юклаб олиш)
7. Malvertising (Нотогри реклама)
8. Rogue Software (Сохта дастурий таъминот)
9. Deep Face
10. Kiber bulling
11. Wardialing

Malware – Электрон қурилмалардан смартфон, компутер, бонкамат ва бошқа қурилмаларга кириб ундан маълумотларни олиб, унга рухсат(доступ) оладиган вируслар, программаларкиради. Бу эмали почталарга, Компутерга юклаб олиш ва Опирацион системага доступ орқали “Зонбий” га айлантириб, ҳоҳлаган вохти кириб маълумтлар олиш ишдан чиқариш, маълумот юбориш, товламачилик қилиши мумкин.

Malware турлари қуйдагилар:

a. Компутер вирус
б. Спйwаре
с. Адwаре
д. Wормс
э. Трожан Ҳорсе

Malware ни нимадан богланиш ёллари:

1. Эмаил почта орқали
2. Программалар сақлаш орқали
3. Операцион система орқали богъланади

Fishing - .енг “Фишинг” – “Балиқ ови” деган маъноларни англатиб, у wеб сайтлар ёки программалар орқали шахсга линк юборади, шахс уни очиб узининг шахсий маълумотларни киритиш орқали, шахсга оид маълумотларни тоъплайди, логини, пароли, wеб сайти, электрон почталарни ва банк картасини маълумотларни олиб, бузишга молжалланган ёъналиш ҳисобланади.

SMS FISHING - мобил телефон сохта шахс ёки юридик шахсдан SMS (Инстант Мессаге ёки IM) олганида юзага келади. Уяли телефондан бехабар фойдаланувчи сохта SMS-хабарга жавоб беради ва УРЛ манзилига ташриф буюради, беихтиёр зарарли дастурни юклаб олади ва фойдаланувчининг хабарисиз троян ўрнатади.

Phishing фойдали маълумотларни олишдан иборат, шунинг учун SMS фишинг ҳолатида троян мобил телефоннинг маълумотлар майдонларини йиғади ва уларни энг эрта имкониятда троянни яратган шахсга узатади. **SMS** фишинг **SMiShing** номи билан ҳам танилган.

SMS фишингга уринишлар мобил телефон фойдаланувчиси номаълум харидни олганлиги ҳақидаги хабарни олувчи бўлганида содир бўлади. Сохта харидларни тўхтатиш ва ойлик ёки кунлик тўловлардан қочиш учун истеъмолчилар фишинг веб-сайтларига йўналтирилади.

Мижозлар билмаган ҳолда тўғридан-тўғри веб-сайтга кириб, хакерларга шахсий мобил телефон маълумотларига киришга имкон беради. Фасебоок каби ижтимоий веб-сайтлар тармоқларида СМС фишинг тобора кенг тарқалган, бу шахсий маълумотларни ўғирлаш усулидир, чунки тасодифан юклаб олинган зарарли дастур барча сақланган мобил телефон маълумотларини, жумладан сақланган кредит карта маълумотларини, исмларни, манзилларни ва электрон почта ҳисоблари учун парол маълумотлари каби бошқа маълумотларни олади ва узатади, улар очилганда, онлайн-банкинг ва бошқа ҳисобларнинг заифлигини ошириш.

Зарарли дастур телефонни, шу жумладан барча қўнғироқлар ёзувларини тозалаш орқали ўз йўлларини ёпиши мумкин, бу эса қайта-қайта ишга тушириш ёки шунга ўхшаш ғалати хатти-ҳаракатларга олиб келади ва телефонни яроқсиз ҳолга келтиради.

Шундай қилиб, оригинал фишинг ҳужуми фойдаланувчи томонидан осонгина сезилмайди. Вируслар ва фишинг фирибгарликлари рақамли қурилмаларнинг барча

турларини қамраб олади. Ақлли истеъмолчилар ўз маҳсулотларини мавжуд маҳсулот хавфсизлиги дастурлари ва маълумотларни қайта тиклаш технологияларига мувофиқ танлашлари керак.

DDOS attacks - компьютер тизимини ишламай қолдириш учун хакерлик ҳужуми, яъни тизимнинг фойдаланувчиларини компутерга зарарли маълумотлар юбориб уни, ишлашини секинлашишга ёки боълмасам бутунлай ишламай қолишига олиб келади, бу эса бошқа кибер ҳужумларни амалга оширишга ёрдам беради.

DOS битта компутер орқали жабирланувчи (жертва)га зарарловчи маълумотларни юбориш ҳисобланади.

DDOS номидан келиб чиқиб 2 ва ундан ортиқ компутер қулмалар орқали жабирланувчи (жертва)га зарарловчи маълумотларни юбориш ҳисобланади, шунда ахборот ресурсларига (серверларга) кириш сустлашади, қотиб қолишига олиб келади.

Бунда катта компаня ва ташкилотлар, сервер ишламай қолишида, бу эса катта миқдордаги зиён етказади. Аммо кўпинча бу иқтисодий босим ўлчовидир: даромад келтирадиган оддий хизматни йўқотиш, провайдердан ҳисоб-китоблар ва ҳужумнинг олдини олиш чоралари нишоннинг чўнтагига сезиларли даражада тегади.

Ҳозирги вақтда DOS ва DDOS ҳужумлари энг оммабоп ҳисобланади, чунки у ҳар витимларни ишлатмай қоъяди, маълумотлар олиш ва уларни бузиш ёълида фойданилади.

Deepfake - бу сохта натижаларни тақдим этиш учун сунъий интеллект ва бошқа замонавий технологиялар ёрдамида такомиллаштирилган видео ва тақдимотлар учун атама.

“Deepfake”нинг энг яхши мисолларидан бири таниқли шахслар, сиёсатчилар ёки бошқалар ҳеч қачон айтмаган ёки қилмаган нарсаларни гапираётгани ёки қилгани ҳақидаги видеони яратиш учун тасвирни қайта ишлашдан фойдаланишни ўз ичига олади. Ижодий медиа белгиси Жордан Пиленинг Youtube даги замонавий тақдимоти Барак Обаманинг сохта видеоларини яратиш учун нисбатан кенг фойдаланиш мумкин бўлган технологиядан фойдаланишни намойиш этади.

Умумий ғоя шундан иборатки, энди ёлғон видео яратиш жуда осон ва бу қисқа муддатда миллий хавфсизлик муаммосига айланиши ёки истеъмолчиларнинг ҳар хил фирибгарликлари ёки бошқа муаммоларга олиб келиши мумкин. Шуни ёдда тутган ҳолда, кенгашлар ва ташкилотлар AI га ахлоқий нуқтаи назардан қандай ёндашишни кўриб чиқмоқдалар, бу чуқур факе ва шунга ўхшаш фирибгарлик ва қўллаб-қувватловчи технологиялар келтириши мумкин бўлган зарарни чеклаш учун.

Kiberbulling - бу ижтимоий тармоқлар, тезкор хабарлар, ўйин платформалари ва мобил телефонларда содир бўлиши мумкин бўлган рақамли зўравонликдир. Бу мақсадни қўрқитиш, ғазаблантириш ёки шарманда қилиш учун мўлжалланган такрорланувчи хатти-ҳаракатлардир.

Kiberbulling мисоллари қуйидагилардан иборат:

- Жабрланувчи тўғрисида нотўғри маълумот тарқатиш ёки ижтимоий тармоқларда нишонга олинган сурат ва видеоларни эълон қилиш;
- Жабрланувчига ҳақоратли ёки таҳдидли хабарлар, тасвирлар ёки видеоларни юбориш;
- Бошқа бировнинг номидан ёки сохта аккаунтлар орқали жабрланувчига ҳақоратли хабарлар юбориш.
- Ҳақиқий ҳаётдаги қўрқитиш ва қўрқитишдан фарқли ўлароқ, кибербуллинг Интернетда рақамли из қолдиради - бу зўравонликни тўхтатишга ёрдам берадиган рекорддир.

АДАБИЕТЛАР:

1. **http:// akadmvd.uz** (Ўзбекистон Республикаси ИИВ Академияси);
2. **http:// lex.uz** (Ўзбекистон Республикаси Қонун ҳужжатлари маълумотлари миллий базаси);
3. **http:// uzsci.net** (Илмий таълим тармоғи);
4. **http:// www.academy.uz** (Ўзбекистон Республикаси Фанлар академияси);
5. **http:// www.ziyonet.uz** (Ахборот таълим тармоғи);
6. **http:// www.uzscience.uz** (Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Фан ва технологияларни ривожлантиришни мувофиқлаштириш қўмитаси);
7. **http:// uzedu.uz** (Ўзбекистон Республикаси Халқ таълим вазирлиги);
8. **http:// www.nuu.uz** (Мирзо Улуғбек номидаги Ўзбекистон миллий университети);
9. **http:// www.tsil.uz** (Тошкент давлат юридик университети);
10. **http:// www.tuit.uz** (Тошкент Ахборот технологиялари университети).