АХБОРОТ ТЕХНОЛОГИЯЛАРИ СОҲАСИДА КИБЕРХАВФСИЗЛИКНИ ТАЪМИНЛАШ ВА ЖИНОЯТЧИЛИККА ҚАРШИ КУРАШИШ УСУЛЛАРИ

Нарзиев Шахзодбек Зойирович
Ўзбекистон Республикаси ИИВ Академияси "Ҳуқуқбузарликлар профилактикаси фаолияти" кафедраси ўқитувчиси, майор
Жолдасов Асилбек Ауезимбет улы
Ўзбекистон Республикаси Ички ишлар вазирлиги Академияси курсанти
E-mail: joldasovasilbek27@gmail.com
https://doi.org/10.5281/zenodo.10539177

АННОТАЦИЯ

Ушбу мақолада замонавий дунёда учрайдиган глабол таҳдидлар ва киберхавфсизлик муаммоси хамда шунинг билан бирга хар бир жамият учун таълим билан бирга бу соҳадаги ахлоқий тарбия ва ахборот маданияти муаммолари муҳим стратегик аҳамиятга эга масалалардан бири атрофлича ўрганилган. Ушбу мақолада киберхавфсизлик, ахборот технологиялар соҳасида содир этилаётган жиноятлар ва уларнинг турлари, тушунчалари мазмуни батафсил баён қилинган. Кибержиноятчиликка карши курашиш бўйича прафилактик ишлар ва чора-тадбирлар амалга оширишда ҳамкорликни кенгайтириш зарурлиги алоҳида қайд этилган.

Калит сўзлар: Киберхавфсизлик, кибержиноятчилик, фишинг,ахборот маданияти, глабаллашув,Global Cybersecurity Index.

ABSTRACT

In this article, the problem of glabol threats and cybersecurity, which is found in the modern world, is studied in detail one of the most important strategic issues of moral education and Information Culture problems in this area, along with education for every society. This article details the content of cybersecurity, crimes committed in the field of Information Technology and their types, concepts. Special mention is made of the need to expand cooperation in the implementation of preventive work and measures to combat cybercrime.

Keywords. Cybersecurity, cybercrime, phishing, information culture, globalization, Global index of cybersecurity

Реал ҳаётда бўлгани каби виртуал дунёда ҳам хавфсизлик муҳим аҳамиятга эга. Дунёда ҳар дақиқада кибермаконда **500 миллион ҳужум** уюштирилади. Киберхавфсизлик стратегиясини тайёрлаган Ўзбекистон ҳам албатта, бу хавф ва хатарлардан хабардор ва бу стратегиядан келиб чиқадиган қоидаларнинг амалга оширилиши уларнинг олдини олишда

муҳим рол ўйнайди. Ўтган даврда Ўзбекистон ҳам киберхавфсизлик индексини яхшилаган. **National cyber security index**[1] давлатларнинг киберхавфсизлик бўйича рейтингини эълон қилди.

Киберхавфсизлик одатда компьютер хавфсизлиги, транзаксия хавфсизлиги, маълумотлар ҳимояси, шахсий маълумотлар хавфсизлиги, интернет тармоғи хавфсизлиги ва ҳаттоки ҳар қандай сигнал узатувчи қурилмалар хавфсизлигини ўз ичига олади. Ушбу мавзуларнинг кенг тарқалиши ва муҳим аҳамият касб этиши сабаби киберҳужумлар ва таҳдидлардир. Киберҳужумлар сони ва тури ошгани сайин киберхавфсизлик тармоқлари ҳам ошиб бормоқда. **1980-йиллардан** бошлаб *“Кибер жиноятчилар”*, *“Кибер дунёда этика”*, *“Ахлоқий кибер қароқчилик”* каби тушунчалар пайдо бўлди. Киберҳужум турлари орасида пул ювиш ва кибержиноятчиларнинг ўз маҳоратини намойиш қилиш учун қилинган ҳужумлари алоҳида ўрин тутади. Киберхавфсизлик киберҳужумларнинг сезиларли даражада ошиши туфайли давлатлар ва компаниялар учун жуда муҳим бўлиб қолди.Шу ўринда ахборот технодлогияларидан фойдаланишнинг бир маданий шакли вужудга келмоқда.Яъни ахборот маданияти тушунчаси секин аста реал ва кибермаконда мухим аҳамият касб ета бошлади.

Ахборот маданияти[2] - эса хабарларни сақлаш, уларнинг аҳамиятли жиҳатларини белгилаб олиш, соҳаларга ажратиш, софлигига эътибор қаратиб муносабат билдириш, ғоявий асосларини аниқлаш, хабар манбаини топишда намоён бўлади. Шунингдек, ахборот маданияти – техник-технологик ва ижтимоий-маданий жиҳатларга эга. Техник-технологик жиҳатдан ахборот маданияти ахборотни олиш, қайта ишлаш ва етказиб беришга хизматларини ўз ичига олиб кетади.

Киберхавфсизлик - бу компьютерлар, серверлар, веб-сайтлар , мобил қурилмалар, электрон тизимлар, тармоқлар ва маълумотларни зарарли ҳужумлардан ҳимоя қилиш амалиётидир. Киберхавфсизлик - бу тизимлар, тармоқлар ва дастурий таъминотни рақамли ҳужумлардан ҳимоя қилиш бўйича чора-тадбирларни амалга оширишдир. Бундай ҳужумлар одатда махфий маълумотларга кириш, уни ўзгартириш, йўқ қилиш, фойдаланувчилардан маблағ олиш, ташкилотлар ёки компанияларнинг нормал фаолиятини бузиш мақсадида амалга оширилади. Киберхавфсизлик бўйича самарали чора-тадбирларни амалга

[1] https://ncsi.ega.ee/ncsi-index/
[2] https://cyberleninka.ru/article/n/ahborot-madaniyati-va-uni-shakllantirishning-nazariy-amaliy-a-amiyati

ошириш аллақачон жуда қийин жараён. Чунки бугунги кунда ҳужумлар амалга оширилаётган қурилмалар сони одамлар сонидан бир неча баробар кўп ва кибержиноятчилар ҳар куни янги ихтиролардан фойдаланмоқда.Ахборот технодогиялар сохасида киберхавфсизликни таъминлашда фойдаланувчилар куйидаги кайд этиб ўтилган билимларга эга бўлиши лозим. Улар куйидагилардан иборат:

- ♣Маълумотлар хавфсизлиги;
- ♣Дастурий таъминот хавфсизлиги;
- ♣Ташкил этувчилар хавфсизлиги;
- ♣Алоқа хавфсизлиги;
- ♣Тизим хавфсизлиги;
- ♣Инсон хавфсизлиги;
- ♣Ташкилот хавфсизлиги;
- ♣Ижтимоий хавфсизлик.

Кибержиноятларнинг кўпайиши давлат бошқаруви, банк, транспорт, миллий хавфсизлик ва бошқа тизимларни такомиллаштириш ва бутун дунё бўйлаб кибермудофаа чораларини кенгайтиришни долзарб қилади. Киберхавфсизлик энг кенг кўламли, глобал ва деярли бутун дунё бўйлаб муаммолардан биридир. Афсуски, самарали киберхавфсизлик чораларини амалга ошириш аллақачон жуда қийин жараён. Чунки бугунги кунда ҳужумлар амалга оширилаётган қурилмалар сони анчагина кўп ва кибержиноятчилар ҳар куни янги ихтиролардан фойдаланмоқда. Кибертаҳдидлар ва киберҳужумлар биз яшаётган ахборот технологиялари асрининг энг катта муаммоларидан бири десак, хато қилмаган бўламиз. Тизимлар, тармоқлар ва дастурий таъминотни рақамли ҳужумлардан ҳимоя қилиш учун киберхавфсизлик чораларини кўриш керак. Ҳозирги замонда кибер жиноятлар сони ортиб бормоқда. Муваффақиятли киберхавфсизлик ёндашуви ҳимоя қилиш учун муҳим бўлган компьютерлар, тармоқлар, дастурлар ёки маълумотларнинг кўп қатламли ҳимояси сифатида аниқланади.

Кибержиноятларнинг кўпайиши давлат бошқаруви, банк, транспорт, миллий хавфсизлик ва бошқа тизимларни такомиллаштириш ва бутун дунё бўйлаб кибермудофаа чораларини кенгайтиришни долзарб қилади. **2012-йилда** АҚШнинг Чикаго шаҳрида бўлиб ўтган НАТО саммитида қабул қилинган якуний маъқуллашда киберҳужумлар сони ва сифати ошиши фактлари яна бир бор тилга олинди ва алянсга аъзо давлатлар алоҳида, шунингдек, халқаро ташкилотлар билан (БМТ, Европа Иттифоқи,

Европа Кенгаши ва бошқалар) ягона кибермудофаа ташкил этиш муҳимлиги таъкидланди.

Бугунги кунда бутун дунё бўйлаб кенг тарқалган хакерлик тармоқлари молиявий операцияларни амалга оширади, фуқароларнинг шахсий маълумотларига киришга эришади, давлат органларининг расмий рақамларини босим остида ушлаб туради. Сўнгги пайтларда баъзи штатлар сайлов тизимига кириш имконига эга бўлгани ҳақида маълумотлар тарқалмоқда. Бу соҳада ташвиқот яратишга уринишлар мавжуд ва шу билан манипуляция имкониятлари кенгаяди. Хакерлар ҳар қандай тизим структурасида тизим хатоларини ёки тизим тешикларини топадилар, улар бу очилиш сабабларини билишади. Киберхавфсизлик бўйича самарали чора-тадбирларни амалга ошириш бугунги кунда жуда қийин, чунки бугунги кунда одамлар кўпроқ қурилмаларга эга бўлишига қарамай, кибержиноятчилар тобора кўпроқ **“ихтирочи”** ролини ўйнамоқда. Шунингдек, бир қатор компьютер фойдаланувчилари **билимсизлик ва эҳтиёцизлик** оқибатида моддий ва маънавий зарар кўрмоқда. Ушбу зарарлардан қочиш учун сиз баъзи асосий мавзуларни билишингиз ва баъзи хавфсизлик чораларини кўришингиз керак.Кибержиноятчиликка қарши кураш уларнинг турларини билиш муҳим аҳамият касб этади ва улардан “**фишинг**” турини кўриб чиқамиз.

Фишинг[3] - бу унда мақсадли электрон почта, телефон ёки матнли хабар орқали қонуний муассаса сифатида намоён бўлган шахс томонидан жисмоний шахсларни шахсий идентификатсиялаш мумкин бўлган маълумотлар, банк ва кредит карта маълумотлари ва пароллар каби махфий маълумотларни тақдим этишга жалб қилиш учун боғланади.

Фишинг ҳужум турлари:[4]

1. **Вейлинг ҳужумлари** (Wҳалинг аттаскс «wҳале» инглизчада кит) – бу «катта ўлжани» яъни ташкилот раҳбарлари ва эгалари ёки медиа ташкилотлари бош муҳаррирларлари каби мансабдор шахсларни нишонга олувчи спир фишинг туридир. Вейлинг ҳужумлари, одатда ҳукумат амалдорлари ёки донор агентликлари каби муҳим ташкилотларнинг ҳамкорлари томонидан юборилган муҳим электрон почта хабарларига ўхшаш бўлган товламачилик электрон почта хабарларини юбориш орқали амалга оширилади.

[3] https://uz.wikipedia.org/wiki/Fishing
[4] https://cyber-star.org/uz/cs-articles/how-to-recognize-phishing-attacks-uz/

2. **СМишинг** СМС хабарлари орқали амалга ошириладиган фишинг туридир. Ушбу ҳужумларни амалга ошираётган фирибгарлар пул ёки шахсий маълумотларингизни олиш учун ўзларини сизнинг танишингиз қилиб кўрсатишлари мумкин. Кўпинча, смишинг ҳужумлар ортидагилар ўзларини тўловни сўраб ёки янгиланишларни таклиф қилиб сизга мурожаат қилувчи сизга хизмат кўрсатадиган хизматлар (масалан, курйерлик компанияси ёки онлайн харид қилиш платформаси) сифатида кўрсатадилар. Кўпинча улар сиз платформа орқали олган тасдиқлаш кодини сўровчи Whatsapp, Facebook ёки бошқа ижтимоий медиа компанияси сифатида сизга мурожаат қилади.

3. **Вишинг** – бу телефон қўнғироқлари орқали амалга ошириладиган фишинг тури. Бундай ҳужумларни амалга оширувчи фирибгарлар ўзларини кўпинча давлат идоралари ходимлари қиёфасида солади. Одатда улар жабрланувчи сўралган маълумотни тақдим этишдан бошқа иложи йўқдек ҳис қилиши учун таҳдид ёки ишонтириш каби усулларидан фойдаланадилар.

Ахборот технололгиялари соҳасида содир этилаётган жиноятчиликка қарши курашда куйидаги усуллар мухим аҳамият касб этади:

Ушбу кибержиноятчиликка карши кураш жараёнида бевосита уни прафилактикаси муҳим аҳамиятга эга ҳисобланиб, ушбу жиноятчилик кўпайган жойларда фойдаланувчиларда ушбу кибержиноятчилик турлари хақида тушунча хосил қилиш, жамоат жойларида ушбу мавзуга дахлдор материалларнни кенг тарғиб етиш самарали усул хисобланади.

Маълумотларни шифрлаш: Маълумотларни енг ичоншли химояси шу усул хисобланиб, бу усулдан фойдаланиш маълумотларнинг ўгирланиши ва уни шикаслантириш олдини олади.

Фақат тўғри коммуникация каналларидан фоидаланиш: электрон почта, телефон, сайтлар ва бошқа коммуникация каналларининг киришда, уларга уланишда ёки улардан фойдаланич жараёнида рухсатларни текчириш, ортиқча рухсатларни олиб ташлаш мақсадга мувофиқ хисобланади.

Фақат расмий иловаларни юклаб олиш: Фақат расмий тарафдан тасдиқланган интернет магазинлари ёки антивируслаштириш компанияларидан илова юклаб олиш керак хисобланиб, бу фойдаланувчиларнинг маълумотлари, хисоблари химояланишини таъминлайди.

Таклиф:

❖ Барча мамлакатларда бўлгани каби Ўзбекистонда ҳам киберхавфсизликка давлат даражасида алоҳида эътибор қаратилмоқда. Таъкидлаш жоизки, Ўзбекистон Республикаси Президентининг 2017 йил 30 июндаги “Республикада ахборот технологиялари соҳасини ривожлантириш учун шарт-шароитларни тубдан яхшилаш чора-тадбирлари тўғрисида”ги пф-5099-сон фармони ва Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2012 йил 19 декабрдаги “Ахборот-коммуникация технологияларини ривожлантириш жамғармасини янада ривожлантириш ва унинг маблағларидан самарали фойдаланиш тўғрисида”ги 356-сон қарори шунингдек, 2020–2023 йилларга мўлжалланган киберхавфсизликка доир миллий стратегия ва “Киберхавфсизлик тўғрисида”ги қонунда белгиланган вазифалардан келиб чиқадиган масалаларни ҳал этиш бўйича ишлар давом эттирилмоқда. Ички ишлар вазирлиги тизимида хам электрон маблағларни талон тарож қилиниши олдини олиш борасида бир қанча ишлар олиб борилмоқда. Чиқарилган қонунлар ижросини таминлаш мақсадида Ички ишлар вазири **генерал-лейтенант П.Р.Бобожонов** ва Тошкент шахар ИИББ бошлиғи **генерал-майор А.А.Ташпўлатов** ташаббуслари билан кибермаконда содир этилаётган жиноятларга қарши курашиш мақсадида Тошкент шахрида *“Ахборот технологиялари сохасидаги жиноятларга қарши курашиш”* бошқармаси ташкил этилди. Хозирги кунда давлатимиздаги мавжуд муаммоларга бархам бериш кибермакондаги жиноятларни олдини олиш мақсадида қатор чора тадбирлар амалга оширилмоқда. Ўзининг тасирини ўтказаётган **фишинг** усулидаги фирибгарликларни олдини олиш мақсадида пойтахтимизнинг қатор масканларида профилактик чора тадбирлар ва давра сухбатлари амалга оширилди. Замон билан хамнафас ривожланиб бораётган интернет ижтимоий тармоқларида блогерлар ва юристлар билан биргаликда тушунтириш ишлари профилактикаси амалга оширилмоқдаХуллас, биринчидан, бугунги кунда дунёдаги илғор киберҳимоя дастурлари ҳар бир фойдаланувчининг манфаатларини ҳимоя қилади. Индивидуал даражада, кибермудофаа ҳужуми шахсий маълумотларнинг ўғирланиши, пул маблағлари ёки оилавий фотосуратлар каби қимматли маълумотларнинг йўқолиши ва кенг миқёсда давлат ва ҳарбий сирларни ошкор қилиш каби салбий оқибатларга олиб келиши мумкин. Электр станциялари, шифохоналар, молиявий хизматлар кўрсатувчи банк сектори

ва бошқа институтлар каби барча муҳим инфратузилмаларни ҳимоя қилиш жамиятимиз ҳаёти ва фаолиятини таъминлаш учун жуда муҳимдир. Иккинчидан, ҳозирда киберхавфсизлик, онлайн хавфсизлик, тармоқлар ишончлилиги учун ҳал қилувчи хавфсизлик масалалари энг муҳим устувор йўналишлардан бири сифатида қаралмоқда. Самарали халқаро ҳамкорлик, кўп томонлама мулоқотга эришиш, ушбу қарорларни муваффақиятли қабул қилиш ва амалга ошириш мақсадида давлат, нодавлат ва халқаро ташкилотлар томонидан ҳар йили минтақавий ва жаҳон миқёсида турли тадбирлар ўтказилмоқда.

Хулоса ўрнида шуни айтиш жойзки, кундан кун ривожланиб бораётган ахборот технологиялари, уларнинг имкониятлари ва ушбу соҳада содир этилаётган жиноятчиликка қарши курашда енг аввало ундан фойдаланувчиларда ахборот маданияти шаклланган булиши лозим. Зеро маълумотлар манбайига айланган интернет тармоғидан ўзига зарур маълумотларни олиши, ундан туғри йулда фойдаланиши керак

Фойдаланган адабиётлар:

1. Киберхавфсизлик, маълумотларни ҳимоя қилиш Ибрагимова Моҳигул Комилжон қизи
2. Ахборот оқими ва ахборот маданиятининг шаклланиш тенденциялари
3. https://uz.wikipedia.org/wiki/Fishing
4. https://cyber-star.org/uz/cs-articles/how-to-recognize-phishing-attacks-uz
5. https://www.imperva.com/learn/application-security/phishing-attack-scam
6. https://cyberleninka.ru/article/n/ahborot-o-imi-va-ahborot-madaniyatining-shakllanish-tendentsiyalari
7. https://newjournal.org/index.php/new/article/download/5228/5003/6709
8. https://news.un.org/ru/story/2021/06/1405532
9. https://rus.lb.ua/economics/2012/01/27/133936_oon_provedet_globalnoe.html
10. https://www.cybercom.mil/Media/News/Tag/47488/cyber/