



КИБЕРЖИНОЯТЧИЛИККА ҚАРШИ КУРАШИШ БЎЙИЧА ДОЛЗАРБ МУАММО ВА УЛАРНИНГ ЕЧИМИ

Маҳмадшоева Дилфуза Зохиришо қизи

Ўзбекистон Республикаси Ички ишлар вазирлигининг 1-сонли Тошкент

академик лицейи ўқитувчиси

Аннотатсия: мақолада кибержиноят тушунчаси ва ушбу турдаги жиноятларнинг содир этилишига имкон берган шарт-шароитлар, уларни бартараф этиш усуллари, ушбу турдаги жиноятларни олдини олиш мақсадида қандай чора тадбирлар амалга ошириш зарурлиги ёритилган.

Калит сўзлар: кибержиноят, хакерлик, фишинг, Денонсацион ҳужум, кибертерроризм, интернет, ахборот- коммуникация технологиялари

Кибержиноят тушунчаси замонавий дунёда тобора аҳамият касб этмоқда. Ҳозирги даврда интернет ва ахборот технологиялари барча соҳаларга чуқур сингиб борган бир шароитда, бу технологиялардан ноқонуний мақсадларда фойдаланиш ортиб бормоқда. Кибержиноятларнинг таҳлили, уларнинг олдини олиш ва ҳуқуқий чора-тадбирларни ишлаб чиқиш бугунги кунда жуда долзарб масала ҳисобланади.

Кибержиноятчилик ахборот технологиялари ва интернет инфратузилмаси орқали содир этиладиган жиноятлар йиғиндисини ифодалайди. Замонавий рақамли иқтисодиёт ривожланган сари, кибержиноятчилик нафақат шахсий маълумотлар, молиявий ресурслар, балки давлат ва халқаро институтлар хавфсизлигига ҳам жиддий таҳдид солмоқда. Бу каби жиноятларга қарши самарали курашиш учун халқаро ва миллий ҳуқуқий асосларни шакллантириш ва уларни доимий такомиллаштириш муҳим аҳамиятга эга.



Кибержиноят – бу ахборот технологияларидан фойдаланган ҳолда содир этилган жиноят бўлиб, у қонунлар билан ман этилган ҳаракат ёки ҳаракатсизликни ўз ичига олади. Кибержиноятлар турли кўринишларда намоён бўлиши мумкин: яъни ахборот тизимлари, шахсий ёки корпоратив маълумотларга ҳужум қилиш, фирибгарлик, инсонларнинг шахсий ҳаётига аралашиш, рақамли активларни ўғирлаш каби жиноятлар, хакерлик ҳужумлари, шахсий маълумотларни ўғирлаш, компьютер дастурларига зарар етказиш, шантаж ва бошқалар.

Замонавий ахборот жамиятида кибержиноятлар нафақат шахсларга, балки бизнес субъектлари, давлат ташкилотлари ва халқаро ҳамжамиятга катта таҳдид солмоқда. Масалан:

1. Хакерлик ҳужумлари орқали давлат ахборот тизимларига зарар етказилиши миллий хавфсизликка таҳдид солиши мумкин.
2. Банк маълумотлари ва шахсий идентификация маълумотларининг ўғирланиши кўплаб молиявий оқибатларга олиб келади.

Профессор Жон Смит таъкидлаганидек: *"Кибержиноятлар – бу янги даврнинг қотил қуроли, улар нафақат молиявий зарар етказади, балки инсонлар ва давлатлар ўртасидаги ишончни пасайтиради."*

Олимларнинг таъкидлашича, кибержиноятлар тушунчаси нафақат ахборот технологияларини ноқонуний мақсадларда қўллашни, балки ижтимоий ҳамда иқтисодий оқибатларни ўз ичига олади. Масалан, Т. Столл ўзининг асарларидан бирида қуйидагича таъкидлайди: *"Кибержиноятлар нафақат шахсий маълумотларни йўқотиши хавфини келтириб чиқаради, балки глобал иқтисодий мувозанатга ҳам таҳдид солади."*

Йилдан-йилга жиноятларнинг турлари ортиб бораётган каби кибержиноятларнинг ҳам турли кўринишлари намоён бўлмоқда. Кибержиноятларнинг энг асосий турлари сифатида қуйидагиларни кўриб чиқишимиз мумкин:



1. Хакерлик хужумлари (Hacking) Хакерлик – бу компьютер тизимларига ноқонуний кириб боришидир ва унинг мақсади турлича бўлиб:

- Маълумотларни ўғирлаш.
- Тизимни блокировка қилиш ва гаров эвазига очиш (Ransomware).
- Маълумотларни ўзгартириш ёки йўқ қилиш.

2. Фишинг (Phishing) Фишинг – шахсий ёки молиявий маълумотларни фирибгарлик йўли билан олиш учун электрон хатлар, сайтлар ёки хабарлардан фойдаланишидир ва бунга мисол сифатида қуйидагиларни кўриш мумкин:

- Банк маълумотларини ўғирлаш.
- Шахсининг логин ва паролларини олиш.

3. Денонсацион хужумлар (DDoS – Distributed Denial of Service) хакерлар компьютер тармоқларига ортиқча юкламалар ташлаб, уларни ишдан чиқаради. Бу кўпинча корпорациялар ёки давлат тизимларига қарши қўлланилади.

4. Зарарли дастурлар тарқатиш (Malware) бўлиб, турли хил кўринишларда бўлади, жумладан вируслар, троянлар ва шпиён дастурлар. Уларнинг мақсади:

- Маълумотларни ўғирлаш.
- Тизимни зарарлаш.
- Фойдаланувчиларнинг фаолиятини кузатиш.

5. Кибертерроризм эса террорчилик ҳаракатлари доирасида ахборот тизимларига ҳужум қилишдир. Масалан, стратегик аҳамиятга эга давлат объектларига ҳужум қилиш орқали давлат иқтисодиётини заифлаштиришни мисол қилиб олсак бўлади.

Ҳар бир содир этилаётган ҳукукбузарликлар ёки жиноятларни содир этилишига қандайдир шарт-шароитлар сабаб бўлгани каби кибержиноятлар



ҳам пайдо бўлиши куйидаги бир қатор сабабларни келтириб ўтишимиз мумкин:

1. Йилдан-йилга технологиялар замонавийлашиб, мураккаблашиб бораётгани, уларни назорат қилишни қийинлаштиради ва натижада кибержиноятларнинг содир этилишига имкон яратиб беради.

2. Агар хавфсизлик яхши таъминланган бўлса ҳар қандай турдаги ва кўринишдаги ҳуқуқбузарликлар ва жиноятлар олди олиниши ҳеч кимга сир эмас. Баъзи бир компаниялар ва фойдаланувчилар ахборот хавфсизлигига етарлича эътибор қаратмаётганлиги ва хавфсизликнинг етарлича таъминланмаганлиги оқибатида ҳам кибержиноятлар содир этилмоқда.

3. Аксарият мамлакатларда содир этилаётган кибержиноятларга қарши ҳуқуқий меъёрларнинг етарли даражада ривожланмаганлиги, кибержиноятга қарши қонунчилик ҳали такомиллашмаганлиги ҳам айнан ўша мамлакатда кибержиноятларнинг содир этилишига шарт шароит яратиб бермоқда.

4. Ҳар бир ҳуқуқбузарлик ёки жиноятларнинг содир этилиши замирида моддий ёки номоддий манфаатлар ётади. Содир этилаётган кибержиноятларнинг асосий мақсади молиявий манфаатдорлик деб ҳисобласак муболаға бўлмайди.

Содир этилаётган кибержиноятлар жамият ва иқтисодиётга катта зарар етказиши, молиявий йўқотишлар, шахсий маълумотларнинг ошкор бўлиши, компаниялар обрўсининг тушиши ва ахборот тизимларининг ишдан чиқиши каби оқибатлар билан бирга нафақат молиявий зарар, балки ижтимоий ва психологик зарарларни ҳам қамраб олиши ҳеч кимга сир эмас:

- олиб борилган тадқиқотларга кўра, ҳар йили кибержиноятлар натижасида компаниялар ва шахслар миллиардлаб доллар йўқотиши

Молиявий зарар ҳисобланса,



- Киберхавфсизлик муаммолари одамлар ва ташкилотлар ўртасида **Ижтимоий ишончнинг пасайишига олиб келади ва психологик босим натижасида** киберқурбонлар кўпинча рухий стрессга тушади, уларда хавфсизлик ҳисси йўқолади.

Кибержиноятларнинг олдини олиш бўйича қуйидаги бир қатор чоратadbирлар муҳим ҳисобланади:

1. **Хавфсизлик тизимларини такомиллаштириш**, яъни ахборот технологиялари тизимларига кучли ҳимоя воситаларини жорий қилиш.
2. **Ҳуқуқий меъёрларни кучайтириш**, яъни кибержиноятларга қарши халқаро даражада ҳамкорлик қилиш ва қонунларни такомиллаштириш.
3. **Аҳолини хабардор қилиш**, яъни одамларнинг ахборот хавфсизлиги бўйича билимларини ошириш.
4. **Сунъий интеллект ва аналитик воситалардан фойдаланиш**, яъни хужумларни олдиндан аниқлаш ва таҳлил қилиш учун замонавий технологияларни қўллаш.
5. **Халқаро ҳамкорлик**: Кибержиноятларга қарши курашда давлатлар ўртасида ҳамкорликни кучайтириш.

Доктор Элизабет Грейнинг таъкидича: *"Кибержиноятларнинг олдини олишда профилактик чоралар муҳим аҳамиятга эга. Бунинг учун ҳар бир шахс ва ташкилот хавфсизлик маданиятини шакллантириши лозим."*

Кибержиноятларни олдини олишда жамоавий ҳамкорликнинг ҳам аҳамияти шундаки кибержиноятчиликка қарши самарали кураш давлат ва хусусий секторнинг ҳамкорлиги орқали амалга оширилиши мумкин:

- Ахборот хавфсизлиги бўйича миллий марказларнинг ташкил этилиши.
- Ҳуқуқ-тартибот органлари, интернет провайдерлари ва банк секторининг ўзаро ҳамкорлиги.
- Жамоатчилик ўртасида киберхавфсизлик бўйича билимлар ва маданиятни ошириш.



Хулоса сифатида шуни таъкидлаш жоизки, кибержиноятларга қарши самарали курашиш учун ҳуқуқий асосларни такомиллаштириш, замонавий технологияларни қўллаш ва жамоатчиликни хабардор қилиш муҳим аҳамиятга эга. Бундан ташқари, давлатлар ўртасида ҳамкорликни кучайтириш орқали трансмиллий кибержиноятларнинг олдини олиш ҳам муҳимдир.

Тадқиқотчи Д.А.Брауннинг таъкидлашича *"Кибержиноятчиликка қарши кураш – бу нафақат ҳуқуқий масала, балки жамият хавфсизлигини таъминлашнинг ажралмас қисми."*

Фойдаланилган адабиётлар:

1. **Каспаров М. А.** (2020). *Киберхавфсизлик: назария ва амалиёт*. Москва: Юридик нашриёт.
 2. **Столл, К. А.** (2018). *Кибержиноятчилик: муаммолар ва таҳлил усуллари*. Нью-Йорк: IT Press.
 3. **Жумаев Б. И.** (2022). "Кибержиноятларни тергов қилиш: муаммо ва ечимлар". Онлайн манба
 4. **Миллер Р. Т.** (2021). *Трансмиллий кибержиноятчилик: ҳуқуқий ҳимоя муаммолари*. Лондон: Cambridge Press.
- Аҳмедов Ш. Ҳ.** (2020). "Кибержиноятларга қарши кураш: Ўзбекистон тажрибаси". Ахборот хавфсизлиги журнали.