ISSN 2181-3187

ИНТЕРНЕТ ТАРМОҒИДА АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ ДАВР ТАЛАБИ

Хасилов Хайрулла Хабибуллаевич
Ўзбекистон Республикаси Ички ишлар вазирлиги
Малака ошириш институти
Махсус-фанлар кафедраси катта ўқитувчиси, подполковник

Аннотация: Ушбу мақола замонавий жамиятда киберхавфсизликнинг ахамияти, асосий таҳдидлар ва уларга қарши ҳимоя чораларини ёритади. Шунингдек, киберхавфсизликка оид тушунчалар, халқаро стандартлар ва Ўзбекистондаги ҳуқуқий нормалар яъни «Киберхавфсизлик тўғрисида»ги, Ахборотлаштириш тизими билан боғлиқ айрим фикрлар илгари сурилган.

Таянч сўзлар: Киберхавфсизлик, Ахборот хавфсизлиги, Кибержиноятлар, Шахсий маълумотлар, Қонунчилик нормалари, Халқаро стандартлар, Суний интеллект (ИИ) каби атама сўларни ўз ичига олади..

Мазкур мақолада муаллиф Янги Ўзбекистон Республикасини барпо этиш ва аҳоли фаровонлигини ҳамда Мамлакат тараққиёти ва барқарорлигини таъминлаш кўп жиҳатдан аҳолининг сиёсий ҳокимиятга ишончи ва жамият ҳаётида қонун устуворлиги ҳамда ижтимоий адолат тамойилларига тўлақонли амал қилиш даражасига боғлиқдир. Республикамизда давлат тузилмаси барча соҳаларда рақамли технологиялардан фойдаланиш билан узвий боғланган. Киберхавфсизлик аслида миллий хавфсизлик, сиесий, иқтисодий ва ижтимой барқарорлик учун ҳам муҳим ўрин тутади. Ҳозирги кунда технологиялар жадал ривожланмоқда ва бу билан бирга киберхавфсизлик ва унда ҳимояланиш масалалари ҳам долзарб бўлиб бормоқда.

Айни кунда интернетга уланган қурилмалар сонининг кўпайиши, маълумотарнинг рақамлаштирилиши ва суний интеллектнинг ҳаётимизга кириб келиши билан киберхавфсизлик нафақат IT мутахассисларининг, балки ҳар бир инсоннинг кундалик муаммосига айланмоқда.

Ахборотлаштириш соҳасидаги давлат сиёсати ахборот ресурслари, ахборот технологиялари ва ахборот тизимларини ривожлантириш ҳамда такомиллаштиришнинг замонавий жаҳон тамойилларини ҳисобга олган ҳолда миллий ахборот тизимини яратишга қаратилган.

ISSN 2181-3187

Мамлакатимизда Ахборотлаштириш тўғрисида қонуннинг 4-моддасида Ахборотлаштириш соҳасидаги қуйидаги тушунчалар келтирилган[1]:

- ҳар кимнинг ахборотни эркин олиш ва тарқатишга доир конституциявий ҳуқуқларини амалга ошириш, ахборот ресурсларидан эркин фойдаланилишини таъминлаш;
- давлат органларининг ахборот тизимлари, тармоқ ва ҳудудий ахборот тизимлари, шунингдек юридик ҳамда жисмоний шахсларнинг ахборот тизимлари асосида Ўзбекистон Республикасининг ягона ахборот маконини яратиш;
- халқаро ахборот тармоқлари ва Интернет жаҳон ахборот тармоғидан эркин фойдаланиш учун шароит яратиш;
- давлат ахборот ресурсларини шакллантириш, ахборот тизимларини яратиш ҳамда ривожлантириш, уларнинг бир-бирига мослигини ва ўзаро алоқада ишлашини таъминлаш;
- ахборот технологияларининг замонавий воситалари ишлаб чиқарилишини ташкил этиш;
- ахборот ресурслари, хизматлари ва ахборот технологиялари бозорини шакллантиришга кўмаклашиш;
- дастурий маҳсулотлар ишлаб чиқариш ривожлантирилишини рағбатлантириш;
- тадбиркорликни қўллаб-қувватлаш ва рағбатлантириш, инвестицияларни жалб этиш учун қулай шароит яратиш;
- кадрлар тайёрлаш ва уларнинг малакасини ошириш, илмий тадқиқотларни рағбатлантириш.

Шу билан биргаликда Ўзбекистон Республикаси Президентининг Сунъий интеллект технологияларини жадал жорий этиш учун шарт-шароитлар яратиш чора-тадбирлари тўғрисида Қарори қабул қилинган.

Мазкур қарорда «Рақамли Ўзбекистон — 2030» Стратегиясига мувофиқ ҳамда сунъий интеллект технологияларини жадал жорий этиш ва уларни мамлакатимизда кенг қўллаш, рақамли маълумотлардан фойдаланиш имкониятини ва уларнинг юқори сифатини таъминлаш, ушбу соҳада малакали кадрлар тайёрлаш учун қулай шарт-шароитлар яратиш мақсади келтирилган[2].

Киберхавфсизлик, тушунчаси ва унга оид тавфсилотлар олимлар томонидан ўрганилган ва таъриф берилган.

[1] Ўзбекистон Республикасининг “Ахборотлаштириш тўғрисида”ги 2003 йил 11 декабрь, 560-II-сон қонуни.

[2] Ўзбекистон Республикаси Президентининг 2021-йил 17-февралдаги ПҚ-4996-сон “Сунъий интеллект технологияларини жадал жорий этиш учун шарт-шароитлар яратиш чора-тадбирлари тўғрисида”ги Қарори.

ISSN 2181-3187

Жумладан: Киберхавфсизлик нима?– бу компьютер тизимлари, тармоқлар ва маълумотларни рухсатсиз кириш, ўзгартириш ёки йўқ қилишдан химоя қилиш бўйича чора-тадбирлар йиғиндиси (Мажмуаси) ҳисобланади.

Киберхавфсизлик қуйидаги асоси йўналишларни ўз ичига олади:

- Тармоқ хавфсизлиги–компьютер тармоқларини хакерлар ва зарарли дастурлардан химоя қилиш.
- Маълумотлар хавфсизлиги–шахсий ва корпоратив маълумотларни сақлаш ва узатиш жараёнида химоя килиш.
- Идентификация ва аутентификация–фойдаланувчини идентификатори орқали таниб олиш жараёни ва рухсат берилган амалларни бошкариш.

Асосий кибер тахдидлар. Қуйида асосий кибер таҳдидлар рўйхатини кенгайтириб, уларнинг моҳияти, зарарлари ва мисоллари ҳақида батафсил маълумот тақдим этилган:

1. Фишингнинг мураккаб шакллари (Spear Phishing)

-Моҳияти:

❖ Одатий фишингдан фарқли равишда, ҳужум шахс ёки ташкилотга мўлжалланган бўлади. Хакерлар қурбоннинг маълумотларини ўрганиб чиқиб, махсус тарзда алданувчи хабарлар юборишади.

-Мақсад:

❖ Банк ҳисоблари, стратегик ҳужжатлар ёки муҳим паролларни қўлга киритиш.

-Мисол:

❖ Компания раҳбарларига сохта инвойс юбориб, молиявий маблағларни ўғирлаш.

-Зарарлари:

❖ Йирик компаниялар ва давлат идораларидаги ҳужумлар оқибатида катта молиявий ва ахборот йўқотишлар содир бўлади.

2. Зиёнловчи интеллектуал дастурлар (Advanced Persistent Threats - APT)

-Моҳияти:

✓ Мақсадли ҳужумлар бир муддат давом эттирилиб, тизимга чуқурроқ сингишга қаратилган бўлади.

-Мақсад:

✓ Давлат ёки корпорациянинг муҳим маълумотларини қўлга киритиш, маълумотларни узоқ муддатда ўғирлаш.

-Мисоллар:

ISSN 2181-3187

✓ 2010 йилдаги Stuxnet ҳужуми, у Эрон ядровий дастурларига зарар етказиш учун яратилган.

-Зарарлари:

✓ Тармоқ тизимларининг хавфсизлигини тўлиқ бузиш ва стратегик маълумотларни назоратга олиш.

3. Криптовалюта билан боғлиқ таҳдидлар (Cryptojacking)

Моҳияти:

✓ Хакерлар қурбоннинг қурилмаларини яширинча криптовалюта қазиб олиш учун ишлатишади.

Мақсад:

✓ Қурбоннинг электр энергияси ва ҳисоблаш ресурсларидан фойдаланиш.

Мисоллар:

✓ CoinHive каби зарарли скриптлар орқали браузерларда яширин криптовалюта қазиб олиш.

Зарарлари:

✓ Тизимнинг ишлаш самарадорлиги пасаяди, қурилмаларга зиён етади.

4. Сунъий интеллектдан хато фойдаланиш (AI-Powered Attacks)

Моҳияти:

✓ Хакерлар сунъий интеллект ёрдамида ҳужумларни автоматлаштиришади ва мураккаблаштирадилар.

Мақсад:

✓ Катта ҳажмдаги маълумотларни таҳлил қилиб, заифликларни топиш.

Мисоллар:

✓ AI ёрдамида мукаммал фишинг хабарлари ёки аудио-тақлид (Deepfake) орқали инсонларни алдаш.

Зарарлари:

✓ Тизимларнинг заиф нуқталаридан фойдаланиб, маълумотларга ноқонуний кириш.

5. Қурилмалар хавфсизлигидаги заифликлар (Hardware Vulnerabilities)

Моҳияти:

✓ Қурилмалардаги техник ёки дастурий заифликлар орқали ҳужум.

Мақсад:

✓ Жисмоний ёки сервер орқали маълумотларга кириш.

Мисоллар:

ISSN 2181-3187

✓ Meltdown ва Spectre (Спектрдаги ҳалокат) каби процессор заифликлари.

Зарарлари:

✓ Фойдаланувчи маълумотларининг очиқланиши ва ресурсларнинг зарарланиши.

6. Ахборотнинг махфийлигини бузиш (Data Breaches)

Моҳияти:

✓ Ҳакерлар маълумотлар базасига кириб, шахсий маълумотларни ўғирлашади.

Мақсад:

✓ Маълумотларни сотиш ёки шантаж қилиш.

Мисоллар:

✓ 2021 йилда Facebookдан 500 миллион фойдаланувчининг маълумотлари ўғирланган.

Зарарлари:

✓ Шахсий ва корпоратив маълумотларнинг махфийлиги бузилади.

7. Рақамли тўлов тизимларига ҳужумлар (Payment Fraud)

Моҳияти:

✓ Онлайн тўлов тизимлари ва банк хизматларига ҳужум қилиш орқали маблағ ўғирлаш.

Мақсад:

✓ Қурбонларнинг молиявий ресурсларини қўлга киритиш.

Мисоллар:

✓ Соҳта тўлов саҳифалари орқали алдаш ёки QR-код орқали ҳужумлар.

Зарарлари:

✓ Одамлар ва компаниялар катта молиявий зарар кўради.

8. Блокчейн ва смарт-шартномалар заифликлари (Blockchain Attacks)

Моҳияти:

✓ Смарт-шартномалардаги хато ёки заифликлардан фойдаланиб ҳужум қилиш.

Мақсад:

✓ Криптовалюталар ёки блокчейн асосидаги дастурлардан маълумотларни олиб қўйиш.

Мисоллар:

✓ 2021 йилда Poly Network (Поли-тармоқ) ҳужуми, унда $610 миллион криптовалюта ўғирланган.

ISSN 2181-3187

Зарарлари:

✓ Молиявий йўқотиш ва тизимларга ишончсизлик.

9. Вақтинчалик ишдан чиқарувчи ҳужумлар (Zero-Day Exploits)

Моҳияти:

✓ Дастур ёки тизимнинг ҳали янгиланмаган заифликларидан фойдаланиш.

Мақсад:

✓ Давлат ёки компания тизимларига кириб, маълумотларни назорат қилиш.

Мисоллар:

✓ Google Chrome ёки Windows каби тизимларда кўплаб заифликлар топилган.

Зарарлари:

✓ Тизимни ишдан чиқариш ёки маълумотларни ўғирлаш.

Хулоса

Асосий кибер таҳдидлар нафақат шахсий фойдаланувчилар, балки компаниялар ва давлат учун ҳам катта хавф солади. Ҳар бир таҳдидга қарши махсус ҳимоя чоралари ишлаб чиқиш ва тизимларни мунтазам янгилаш муҳим аҳамиятга эга. Ўзбекистон Республикасида киберхавфсизликни таъминлашга қаратилган қонунчилик асослари бир қатор қонунлар, фармонлар ва қарорлар орқали шакллантирилган. Улар ахборот хавфсизлиги ва киберҳимоя бўйича давлат сиёсатининг муҳим йўналишларини белгилайди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Ўзбекистон Республикаси янги таҳрирдаги Конституцияси. Т-.2023
2. Ўзбекистон Республикасининг янги таҳрирдаги Конституцияси. 2023 й. https://lex.uz/docs/6445145
3. Ўзбекистон Республикасининг 2003-йил 11-декабрдаги “Ахборотлаштириш тўғрисида”ги ЎРҚ-560-II-сонли Қонуни. https://lex.uz/docs/83472
4. Ўзбекистон Республикаси Президентининг 2021-йил 17-февралдаги ПҚ-4996-сон “Сунъий интеллект технологияларини жадал жорий этиш учун шарт-шароитлар яратиш чора-тадбирлари тўғрисида”ги Қарори. https:// https://lex.uz/uz/docs/5297046
5. Ўзбекистон Республикасининг 2022-йил 15-апрелдаги “Киберхавфсизлик тўғрисида”ги ЎРҚ-764-II-сонли Қонуни. https://lex.uz/uz/docs/5960604
6. Ўзбекистон Республикаси Президентининг 2022-йил 6-июлдаги ПФ-165-сон “2022 — 2026 йилларда Ўзбекистон Республикасининг инновацион ривожланиш стратегиясини тасдиқлаш тўғрисида” Фармони. https://lex.uz/docs/6102462
7. Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг Олий Мажлис ва Ўзбекистон халқига Мурожаатномаси 2022 йил.