



КИБЕРЖИНОЯТЛАР УЧУН ЖИНОЙ ЖАВОБГАРЛИК: ҚИЁСИЙ- ҲУҚУҚИЙ ТАҲЛИЛ

Ҳикматов Абдурасул Анвар ўғли
Ўзбекистон Республикаси Ҳуқуқни
муҳофаза қилиш академияси “Тергов
фаолияти” йўналиши магистранти
Тел: +998933122222
E-mail: hikmatov94@inbox.ru

Аннотация: Ушбу мақолада кибержиноятлар учун жиноий жавобгарлик масалалари қиёсий-ҳуқуқий жиҳатдан таҳлил қилинган. Турли мамлакатларнинг қонунчилиги ўрганилиб, кибержиноятларга қарши курашиш бўйича халқаро тажриба таҳлил этилган. Миллий қонунчиликни такомиллаштириш юзасидан таклиф ва тавсиялар ишлаб чиқилган.

Калит сўзлар: кибержиноят, жиноий жавобгарлик, компьютер жиноятлари, киберхавфсизлик, халқаро ҳамкорлик.

Аннотация: В данной статье с сравнительно-правовой точки зрения анализируются вопросы уголовной ответственности за киберпреступления. Изучено законодательство различных стран и проанализирован международный опыт борьбы с киберпреступлениями. Разработаны предложения и рекомендации по совершенствованию национального законодательства.



Ключевые слова: киберпреступление, уголовная ответственность, компьютерные преступления, кибербезопасность, международное сотрудничество.

Abstract: This article analyzes the issues of criminal liability for cybercrimes from a comparative legal perspective. The legislation of various countries has been studied, and international experience in combating cybercrimes has been analyzed. Proposals and recommendations have been developed to improve national legislation.

Keywords: cybercrime, criminal liability, computer crimes, cybersecurity, international cooperation.

Замонавий дунёда ахборот технологияларининг жадал ривожланиши билан бирга кибержиноятлар сони ҳам тобора ортиб бормоқда. Бу эса ўз навбатида кибержиноятларга қарши курашиш ва уларни олдини олиш масалаларини долзарб қилиб қўймоқда. Кибержиноятлар нафақат алоҳида шахсларга, балки бутун жамият ва давлат манфаатларига жиддий таҳдид солмоқда.

Буни қуйидаги рақамлар ҳам кўрсатиб турибди. Хусусан, 2023 йил бошида глобал кибержиноятлардан кўрилган зарар тахминан 8 триллион АҚШ долларини ташкил этган. Кибержиноятларнинг асосан қуйидаги турлари содир этилган: фишинг ҳужумлари - 36%, маълумотларни ўғирлаш - 27%, шифрлаш орқали товламачилик - 21%, DDoS ҳужумлари - 16%¹.

Ўзбекистонда кибержиноятлар сони сўнгги йилларда сезиларли даражада ошган. 2020 йилда ахборот технологиялари соҳасида 106 та жиноят қайд этилган бўлса, бу кўрсаткич 2021 йилда 2 281 тага, 2022 йилда 4 332 тага етиб, 2020 йилга

¹ <https://www.interpol.int/content/download/22267/file/INTERPOL%20Annual%20Rep>



нисбатан 40 баравар ошган². Шу сабабли, бугунги кунда кибержиноятларнинг турларини аниқлаш, улар учун жиноий жавобгарликни белгилаш ва олдини олиш тобора долзарб мавзу бўлиб бормокда.

“Кибержиноят” тушунчасига бугунги кунда бир қатор олимлар томонидан турли тушунчалар берилган. Мазкур тураги жиноятлар бошқа турдаги жиноятлардан жиноят содир этиш қуроли, предмети, жойи ва усуллари билан фарқ қилади. Шунингдек, хорижий давлатларда технологик жараёнларнинг ривожланиш даражасига қараб кибержиноятларнинг турли шакллари ва усуллари пайдо бўлмокда.

Рус ҳуқуқшуноси В.Б. Вехов таърифига кўра: “Кибержиноят - бу компьютер ахборотини қайта ишлаш қоидаларини бузиш орқали содир этиладиган ижтимоий хавфли қилмиш бўлиб, унинг объекти сифатида компьютер хавфсизлиги соҳасидаги ижтимоий муносабатлар тушунилади”³.

Профессор Susan W. Brenner “Кибержиноят - бу компьютер тизимлари ва тармоқларидан фойдаланган ҳолда содир этиладиган жиноий фаолият бўлиб, унинг мақсади молиявий фойда олиш ёки тизимларга зарар етказишдир”⁴ – деб таъриф берган.

David S. Wallнинг фикрича “Кибержиноят - бу рақамли технологиялар ёрдамида содир этиладиган трансмиллий характердаги жиноят бўлиб, у анъанавий жиноятлардан ўзининг глобал хусусияти билан фарқ қилади”⁵.

² <https://stat.prokuratura.uz>

³ “Компьютерные преступления: способы совершения и раскрытия”. Монография. В.Б. Вехов - М. : Право и Закон, 1996. 14-бет.

⁴ “Cybercrime: Criminal Threats from Cyberspace” Susan W. Brenner (2010) https://ecommons.udayton.edu/cgi/viewcontent.cgi?article=1023&context=law_fac_pub

⁵ “Cybercrime: The Transformation of Crime in the Information Age”. David S. Wall (2007) https://www.researchgate.net/profile/David-Wall-7/publication/378013252_Cybercrime_The_Transformation_of_Crime_in_the_Information_Age_2nd_edition/links/65c36f3179007454976a5420/Cybercrime-The-Transformation-of-Crime-in-the-Information-Age-2nd-edition.pdf



Бундан ташқари, рус олимлари Д.В. Добровольский, Ю.М. Батурин, М.А. Ефремова, К.Н. Евдокимовлар ҳам ўзларининг илмий ишларида мазкур тушунчага турли таърифлар беришган.

Юқоридаги олимларнинг фикрларини умумлаштириб, кибержиноятларнинг асосий белгилари сифатида ахборот технологияларидан фойдаланиш, ижтимоий хавфлилик, ҳуқуққа хилофлик, трансчегаравий хусусият, компьютер тизимлари ва маълумотларига қарши қаратилганлик ҳамда қасддан содир этилиш кабиларни киритиш мумкин.

Кибержиноят компьютер тизимлари, тармоқлари ва маълумотлар базаларига ноқонуний кириш орқали содир этиладиган жиноий ҳаракатлар ҳисобланади. Мазкур турдаги жиноятларнинг анъанавий жиноятлардан бир неча ўзига хос жиҳатлар билан фарқ қилади:

- Анъанавий жиноятлардан фарқли равишда кибержиноятлар виртуал муҳитда содир этилади;
- Жиноят содир этган шахснинг анонимлиги юқори бўлади;
- Бир вақтнинг ўзида бир неча шахслар жабрланиши мумкин;
- Жиноятларни содир этиш учун махсус билим (дастурий таъминотлар билан боғлиқ) талаб этилади;
- Жиноятнинг изларини тез йўқотиш мумкин ва уни тиклашнинг имкони бўлмайди.

Кибержиноятларнинг содир этилишининг тарихини шартли равишда 5 босқичга бўлиш мумкин.

Биринчи босқич (1970–1980-йиллар) – мазкур даврда илк компьютер ва телефон технологиялари пайдо бўлган давр бўлиб, мазкур даврда асосан Европа давлатлари ва АҚШ да телефон тизимларини бузиш ва дастлабки компьютер ҳужумлари орқали кибержиноятлар содир этилган. Бу даврда содир этилган кибержиноятлар асосан



фирибгарлик кўришинида ва вирусли дастурларни тарқатиш орқали компьютерларга зарар етказиш кўринишларида содир этилган.

Иккинчи босқич (1990–2000-йиллар) – мазкур давр интернетнинг пайдо бўлиши ва у орқали кибержиноятлар содир этилиши билан алоҳида ажралиб туради. Мазкур даврда интернет оммалашishi билан онлайн фирибгарлик, шахсий маълумотларни ўғирлаш ва банк тизимларига хужумлар авж олди. Мазкур даврда дастлабки банк хисобварақларидаги маблағларни ўғирлаш содир этила бошланди.

Учинчи босқич (2000–2010-йиллар) - кибержиноятларнинг глобал тахдидга айланиши даври бўлди. Мазкур даврга келиб, банк карталари, электрон почта хужумлари ва зарарли дастурлар орқали йирик жиноятлар содир этила бошланди. Шунингдек, мазкур даврда онлайн савдо дўконларининг ташкил этиши, банк тизимининг халқаро тармоққа уланиши ва интернет орқали хисобларни бошқариш тизимининг яратилиши кибержиноятларнинг глобал тарзда содир этилишига имкон яратиб берди.

Тўртинчи босқич (2010–2020-йиллар) – мазкур давр бутун дунёда рақамли иқтисодиётга ўтиш даври бўлганлиги сабабли кибержиноятларнинг тахдиди янада ортиб борди. Бу даврга келиб, давлатларнинг иқтисодиётлари рақамлаштириш бошланди. Кибержиноятлар тўғридан тўғри давлатларга, ҳукуматларга қаратила бошланди. Мазкур даврда “кибертерроризм” атамаси вужудга келди.

Бешинчи босқич (2020 йиллардан ҳозирги кунга қадар) – сунъий интеллектнинг яратилиши кибержиноятларни содир этилишини осонлаштирди. Шунингдек, блокчейн ва криптовалюталар вужудга келди. Мазкур воситаларнинг вужудга келиши кибержиноятларни фош этиш, уларни исботлаш ва тергов қилишни янада мураккаблаштирди. Мазкур воситалар натижасида бугунги кунда мамлакатлар ва йирик компаниялар иқтисодиётига миллиардлаб доллар зарар етказиш орқали кибержиноятлар содир этилмоқда.



Бугунги кунда кибержиноятлар компьютер тизимларига рухсатсиз кириш, компьютер маълумотларини ўғирлаш, кибер товламачилик, компьютер вируслари тарқатиш, фишинг ва идентификация маълумотларини ўғирлаш, интернет орқали фирибгарлик ва бошқа турли усуллар билан содир этилмоқда.

Ўзбекистон Республикасида ҳам замонавий ахборот технологиялари ривожлангани сари кибержиноятларнинг тури ва салмоғи ҳам ортиб бормоқда.

Шу сабабли, Ўзбекистон Республикаси Жиноят кодексига бир қатор кибержиноятлар билан боғлиқ номалар киритилган.

Хусусан, Жиноят кодексида ахборот тизимларидан фойдаланиб содир этиладиган шахсий маълумотлардан ноқонуний фойдаланиш, электрон тўлов воситалари ва ахборот тизимларидан фойдаланган ҳолда фирибгарлик, ахборот хавфсизлиги қоидаларини бузиш каби жиноятлар учун жиноий жавобгарлик белгиланган.

Шунингдек, маъмурий жавобгарлик ҳақида ҳам нормалар мавжуд бўлиб, улар оғирлашган ҳолларда жиноий жавобгарликка айланиши мумкин.

Кибержиноятларга қарши курашишда АҚШ, Европа Иттифоқи ва Россиянинг ҳукукий тажрибалари муҳим аҳамиятга эга. Мисол учун, АҚШда 1986 йилда қабул қилинган “Компьютер фирибгарлиги ва суиистеъмоли тўғрисида” ги қонун (Computer Fraud and Abuse Act)га кўра, киберхужумлар, маълумотлар ўғирланиши ва фирибгарлик учун қаттиқ жазо чоралари белгиланган⁶.

Шунингдек, 2001 йилдаги Будапешт конвенцияси Европа Иттифоқи давлатларида кибержиноятларга қарши курашишнинг асосий тамойилларини белгилаб берган. Мазкур конвенцияга мувофиқ, иштирокчи давлатлар кибержиноятларга қарши қонунчиликни уйғунлаштириш мажбуриятини оладилар.

⁶ https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act



Россия Федерациясининг Жиноят кодексида ахборот хавфсизлигига ва кибержиноятларга қарши жиноятлар учун бир нечта моддалар мавжуд.

Хусусан, компьютер маълумотларига ноқонуний кириш, зарарли дастурий таъминот яратиш, тарқатиш ёки қўллаш, компьютер тизими қоидаларини бузиш, электрон воситалардан фойдаланган ҳолда фирибгарлик, тўлов воситалари билан боғлиқ ноқонуний ҳаракатлар, шахсий маълумотларни ноқонуний тўплаш ва тарқатиш, бузғунчи контент яратиш ва тарқатиш кабилар шулар жумласидандир⁷.

Ўзбекистондаги кибержиноятларга оид қонунчилик хорижий тажрибалар билан солиштирилганда, Ўзбекистон Республикаси Жиноят қонунчилиги кибержиноятлар учун жавобгарликни белгилаш соҳасида бир қатор ўзгартириш ва қўшимчаларга киритишга муҳтожлиги кўринади.

Зеро, бугунги кунда ахборот технолгиялари билан боғлиқ муносабатлар жамиятда тобора ривожланиб, кибержиноятларнинг янги турлари пайдо бўлмоқда.

Хусусан, Ўзбекистон Республикаси Жиноят кодексига кибержиноятлар тушунчасини киритиш, зарарли дастурий таъминот яратиш, тарқатиш ёки қўллаш, бузғунчи контент яратиш ва тарқатиш билан боғлиқ ҳаракатлари учун жиноий жавобгарлик белгилаш билан боғлиқ ўзгартириш ва қўшимчалар киритиш зарур.

Сабаби, бугунги кунда ахборот технологияларининг ривожланиб бориши улар орқали содир этиладиган жиноятларнинг турлари ва усулларини кўпайтириб бормоқда. Айниқса, бу медиамаконда, иқтисодиёт тармоқларида яққол намоён бўлиб бормоқда. Шу сабабли, Ўзбекистон Республикаси Жиноят кодексига ўз вақтида тегишли ўзгартириш ва қўшимчалар киритиб бориш зарур.

Хулоса қилиб айтганда, кибержиноятлар бугунги глобал таҳдид бўлиб, уларга қарши самарали курашиш учун қонунчиликни такомиллаштириш ва халқаро ҳамкорликни кучайтириш зарур.

⁷ https://www.consultant.ru/document/cons_doc_LAW_10699/



Ўзбекистонда бу соҳада муайян ижобий ўзгаришлар кузатилмоқда, бироқ, ҳали кўплаб камчиликлар мавжуд. Киберхавфсизликни ошириш, фуқароларни ҳимоя қилиш ва халқаро стандартларга мос қонунчилик яратиш – бугунги куннинг энг долзарб вазифаларидан биридир.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ:

1. Ўзбекистон Республикаси Конституцияси.
2. Ўзбекистон Республикаси Жиноят кодекси.
3. Ўзбекистон Республикасининг “Ахборотлаштириш тўғрисида”ги Қонуни.
4. Ўзбекистон Республикасининг “Ахборот хавфсизлиги тўғрисида”ги Қонуни.
5. Будапешт Конвенцияси "Convention on Cybercrime" (2001).
<https://www.coe.int/en/web/cybercrime/the-budapest-convention>
6. АҚШ Компьютер фирибгарлиги ва суиистеъмоли тўғрисидаги Қонун (CFAA, 1986).
7. Европа комиссиясининг кибержиноятлар ва хавфсизлик бўйича ҳисоботи (Cybercrime and Security Report) 2022 йил. <https://www.europol.europa.eu/report-a-crime/report-cybercrime-online>
8. В.Б. Вехов. Информационное право и киберпреступления. Москва, 2020 йил.
9. Susan W. Brenner. Cybercrime: Criminal Threats from Cyberspace. New York, 2010.
10. David S. Wall. Cybercrime: The Transformation of Crime in the Information Age. Cambridge, 2007.
11. Д.В. Добровольский, Ю.М. Батурин, М.А. Ефремова, К.Н. Евдокимов. Киберпреступность и цифровая безопасность. Москва, 2019 йил.
12. Россия Федерациясининг Жиноят кодекси.
13. Transparency International. Кибержиноятлар ва Коррупция Ҳисоботи 2023.
<https://www.reportlinker.com/market-report/Cybersecurity/517797>