КИБЕРЖИНОЯТЛАР ВА УЛАР УЧУН ЖИНОИЙ ЖАВОБГАРЛИКНИ ТАКОМИЛЛАШТИРИШ МАСАЛАЛАРИ.

Мамутов Баходир
Бердақ номидаги Қорақалпоқ
давлат университети стажёр ўқитувчиси
https://doi.org/10.5281/zenodo.20911812

Аннотация

Ушбу мақолада кибержиноятлар тушунчаси, уларнинг асосий турлари ва жамият учун хавфли жиҳатлари таҳлил қилинган. Ахборот технологияларининг жадал ривожланиши натижасида компьютер тизимларига ноқонуний кириш, интернет фирибгарлиги, шахсий маълумотларни ўғирлаш каби жиноятлар сони ортиб бормоқда. Мақолада Ўзбекистон Республикаси жиноят қонунчилигида кибержиноятлар учун назарда тутилган жавобгарлик чоралари ўрганилиб, уларни такомиллаштириш масалалари кўриб чиқилган. Шунингдек, халқаро тажриба таҳлили асосида кибержиноятларга қарши курашиш самарадорлигини ошириш, рақамли далиллардан фойдаланиш ва ҳуқуқни муҳофаза қилувчи органлар фаолиятини такомиллаштириш бўйича таклифлар берилган.

Annotation

This article analyzes the concept of cybercrime, its main types, and the threats it poses to society. The rapid development of information technologies has led to a significant increase in crimes such as unauthorized access to computer systems, internet fraud, and the theft of personal data. The article examines the criminal liability established for cybercrimes under the legislation of the Republic of Uzbekistan and discusses issues related to its improvement. Furthermore, based on an analysis of international experience, proposals are presented to enhance the effectiveness of combating cybercrime, improve the use of digital evidence, and strengthen the activities of law enforcement agencies in this field.

Аннотация

В данной статье анализируются понятие киберпреступности, её основные виды и общественная опасность. Стремительное развитие информационных технологий приводит к росту числа таких преступлений, как несанкционированный доступ к компьютерным системам, интернет-мошенничество и хищение персональных данных. В статье рассматриваются меры уголовной ответственности за киберпреступления, предусмотренные законодательством Республики Узбекистан, а также вопросы их совершенствования. Кроме того, на основе анализа

международного опыта предлагаются меры по повышению эффективности борьбы с киберпреступностью, совершенствованию использования цифровых доказательств и деятельности правоохранительных органов в данной сфере.

Калит сўзлар: кибержиноят, киберхавфсизлик, жиноий жавобгарлик, ахборот хавфсизлиги, компьютер жиноятлари, интернет фирибгарлиги, рақамли далиллар, шахсий маълумотлар, киберҳужумлар, рухсатсиз кириш, ахборотни ҳимоя қилиш, ахборот технологиялари, ҳуқуқни муҳофаза қилувчи органлар, рақамли муҳит, халқаро ҳамкорлик.

Keywords: Cybercrime, cybersecurity, criminal liability, information security, computer crimes, internet fraud, digital evidence, personal data, cyberattacks, unauthorized access, information protection, information technologies, law enforcement agencies, digital environment, international cooperation.

Ключевые слова: Киберпреступность, кибербезопасность, уголовная ответственность, информационная безопасность, компьютерные преступления, интернет-мошенничество, цифровые доказательства, персональные данные, кибератаки, несанкционированный доступ, защита информации, информационные технологии, правоохранительные органы, цифровая среда, международное сотрудничество.

Ҳозирги кунда ахборот-коммуникация технологияларининг жадал ривожланиши ва жамият ҳаётининг рақамлашуви инсон фаолиятининг деярли барча соҳаларига сезиларли таъсир кўрсатмоқда. Интернет тармоғи, электрон тўлов тизимлари, булутли технологиялар ва сунъий интеллектга асосланган хизматларнинг кенг қўлланилиши иқтисодий ва ижтимоий муносабатларни янги босқичга олиб чиқди. Шу билан бирга, рақамли технологияларнинг оммалашуви янги турдаги ҳуқуқбузарликлар, хусусан, кибержиноятларнинг кўпайишига ҳам сабаб бўлмоқда.

Кибержиноятлар ахборот тизимлари, компьютер тармоқлари ва рақамли маълумотларга қарши қаратилган ёки улардан фойдаланган ҳолда содир этиладиган жиноий қилмишлар ҳисобланади. Бундай жиноятлар қаторига компьютер тизимларига ноқонуний кириш, зарарли дастурларни тарқатиш, интернет фирибгарлиги, шахсий маълумотларни ўғирлаш, электрон тўлов воситаларидан ноқонуний фойдаланиш ва бошқа турдаги ҳуқуқбузарликлар киради. Уларнинг трансмиллий хусусиятга эга эканлиги, қисқа вақт ичида катта миқдорда зарар етказиши ҳамда жиноятчиларни

аниқлашнинг мураккаблиги мазкур соҳада ҳуқуқий тартибга солиш механизмларини доимий такомиллаштириб боришни талаб этади.

Сўнгги йилларда Ўзбекистон Республикасида ҳам рақамли иқтисодиётни ривожлантириш, давлат хизматларини электрон шаклга ўтказиш ва ахборот хавфсизлигини таъминлашга қаратилган кенг кўламли ислоҳотлар амалга оширилмоқда. Бироқ ахборот технологияларининг ривожланиши билан бир қаторда кибержиноятлар сони ва уларнинг ижтимоий хавфлилик даражаси ҳам ортиб бормоқда. Мазкур ҳолат кибержиноятлар учун жиноий жавобгарлик чораларининг самарадорлигини баҳолаш ва уларни такомиллаштириш заруратини юзага келтирмоқда.

Ушбу мақоланинг мақсади кибержиноятлар тушунчаси ва турларини таҳлил қилиш, улар учун назарда тутилган жиноий жавобгарликнинг ҳуқуқий асосларини ўрганиш ҳамда халқаро тажриба асосида миллий қонунчиликни такомиллаштириш бўйича таклиф ва тавсиялар ишлаб чиқишдан иборат.

Муҳокама ва натижалар

Кибержиноятлар бугунги глобаллашув ва рақамли трансформация шароитида жиноят ҳуқуқининг энг долзарб йўналишларидан бирига айланган. Ахборот-коммуникация технологияларининг кенг жорий этилиши натижасида жамиятнинг барча соҳалари рақамли муҳитга ўтди, бу эса ўз навбатида янги турдаги ҳуқуқбузарликлар – кибержиноятларнинг кескин ортишига сабаб бўлди. Ўзбекистон Республикасининг Жиноят кодексида ахборот технологиялари соҳасидаги жиноятлар учун махсус нормалар белгиланган бўлиб, улар XX[1] боб (278[1]–278[9]-моддалар) доирасида тартибга солинади[1].

Мазкур нормаларнинг жорий этилиши кибержиноятларга қарши ҳуқуқий курашни мустаҳкамлашга хизмат қилган бўлса-да, амалиётда ушбу жиноятларнинг мураккаблиги, трансчегаравий хусусияти ва технологик тезкор ривожланиши мавжуд қонунчиликни доимий такомиллаштириш заруратини юзага келтирмоқда. Хусусан, кибержиноятлар нафақат мулкий зарар етказади, балки шахсий маълумотларнинг бузилиши, давлат хавфсизлигига таҳдид ва иқтисодий тизимга ишончнинг пасайишига ҳам олиб келади[2].

[1] Ўзбекистон Республикаси Жиноят кодекси. – Lex.uz, 278[1]–278[9]-моддалар.
[2] “Киберхавфсизлик тўғрисида”ги Ўзбекистон Республикаси Қонуни. – Lex.uz.

Ўзбекистон Жиноят кодексида кибержиноятлар алоҳида бобда берилган бўлса-да, амалиётда уларни квалификация қилишда бир қатор муаммолар мавжуд. Масалан, компьютер тизимларига рухсатсиз кириш натижасида амалга оширилган фирибгарлик ҳаракатлари кўпинча 168-модда (фирибгарлик) билан бирга 278[1]-модда билан ҳам квалификация қилинади[3]. Бу эса жиноят таркибини тўғри аниқлашда қийинчилик туғдиради.

Шунингдек, кибержиноятларнинг кўплаб ҳолатлари анонимлик, VPN, darknet ва криптовалюталар орқали амалга оширилгани сабабли жиноятчини аниқлаш ва исботлаш жараёни мураккаблашмоқда. Бу ҳолат жиноят-процессуал нормаларни ҳам такомиллаштириш заруратини келтириб чиқаради.

Ўзбекистон Республикаси Жиноят кодекси кибержиноятларга оид қуйидаги асосий таркибларни белгилайди: компьютер ахборотини ноқонуний эгаллаш ёки ўзгартириш (278[1]-модда), компьютер тизимларига рухсатсиз кириш (278[2]-модда), зарарли дастурлар яратиш ва тарқатиш (278[3]-модда), ахборот тизимларини бузиш (278[4]-модда)[4].

Ушбу нормалар Европа Кенгашининг Будапешт конвенцияси тамойилларига ҳамоҳанг бўлиб, халқаро стандартларга мос келади. Бироқ замонавий кибержиноят турларининг тез ривожланиши (phishing, social engineering, deepfake фирибгарлиги) мавжуд нормаларда тўлиқ қамраб олинмаган.

Кибержиноятларни тергов қилишда асосий муаммолардан бири рақамли далилларнинг йиғилиши ва уларнинг ҳуқуқий мақомини аниқлаш ҳисобланади. Рақамли далиллар (лог файллар, IP манзиллар, электрон ёзишмалар) осон ўзгартирилиши ёки йўқ қилиниши мумкин. Шу сабабли “chain of custody” тамойилини жорий этиш мақсадга мувофиқдир[5].

Халқаро тажрибада, жумладан АҚШ ва Европа давлатларида кибержиноятларга қарши махсус қонунчилик ва техник стандартлар ишлаб чиқилган. Бу эса миллий қонунчиликни такомиллаштиришда муҳим аҳамият касб этади.

Шунингдек, кибержиноятлар учун жиноий жавобгарликни кучайтириш фақат жазони оғирлаштириш билан чекланмаслиги керак, балки профилактика, ахборот хавфсизлиги маданиятини ошириш ва

[3] Ўзбекистон Республикаси Жиноят кодекси, 168-модда (Фирибгарлик). – Lex.uz.
[4] Council of Europe. Budapest Convention on Cybercrime, 2001.
[5] Criminal Justice Handbook on Digital Evidence. UNODC, 2022.

фойдаланувчиларнинг рақамли саводхонлигини юксалтириш ҳам муҳим ҳисобланади.

Хулоса

Кибержиноятлар ва улар учун жиноий жавобгарликни такомиллаштириш масалалари юзасидан ўтказилган таҳлиллар шуни кўрсатадики, ахборот-коммуникация технологияларининг жадал ривожланиши жиноят ҳуқуқи тизими олдига мутлақо янги вазифаларни қўймоқда. Рақамли иқтисодиётнинг кенгайиши, электрон тўлов тизимларининг оммалашиши, давлат хизматларининг онлайн шаклга ўтиши ҳамда ахборот алмашинувининг глобал тармоқлар орқали амалга оширилиши кибержиноятлар учун кенг имкониятлар яратмоқда. Шу сабабли мазкур турдаги жиноятлар нафақат миллий, балки халқаро хавфсизликка ҳам жиддий таҳдид солувчи омилга айланиб бормоқда.

Тадқиқот давомида аниқландики, Ўзбекистон Республикаси Жиноят кодексида кибержиноятларга оид махсус нормаларнинг мавжудлиги ҳуқуқий асосларни шакллантирган бўлса-да, улар замонавий киберхавфларни тўлиқ қамраб ололмаяпти. Хусусан, phishing, social engineering, deepfake технологиялари орқали содир этиладиган фирибгарликлар, криптовалюта билан боғлиқ жиноятлар ҳамда сунъий интеллектдан фойдаланган ҳолда амалга ошириладиган ҳуқуқбузарликлар амалдаги нормаларда аниқ тартибга солинмаган. Бу эса қонунчиликни такомиллаштириш заруратини кучайтирмоқда.

Шу билан бирга, кибержиноятларни квалификация қилиш ва тергов қилиш жараёнида бир қатор амалий муаммолар мавжудлиги ҳам аниқланди. Жумладан, бир ҳаракатнинг бир вақтнинг ўзида бир неча моддалар билан квалификация қилиниши, рақамли далилларнинг йўқолиши ёки ўзгартирилиши, IP манзиллар орқали шахсни аниқлашнинг қийинлиги ҳамда халқаро платформалар билан ахборот алмашинувининг чекланганлиги шулар жумласидандир. Бу ҳолатлар тергов органлари фаолияти самарадорлигини пасайтиради ва исботлаш жараёнини мураккаблаштиради.

Таҳлиллар натижасида шу нарса ҳам ойдинлашдики, кибержиноятларга қарши курашиш фақат жиноий жазоларни кучайтириш билан чекланмаслиги лозим. Бу соҳада комплекс ёндашув, яъни профилактика, ахборот хавфсизлиги маданиятини ошириш, фуқароларнинг рақамли саводхонлигини юксалтириш ва техник ҳимоя тизимларини такомиллаштириш муҳим аҳамият касб этади. Чунки кўплаб

кибержиноятлар инсон омили, яъни фойдаланувчиларнинг эҳтиётсизлиги ва ахборот саводхонлигининг етарли эмаслиги натижасида содир этилмоқда.

Шунингдек, халқаро тажрибани ўрганиш натижасида кибержиноятларга қарши курашда трансчегаравий ҳамкорликнинг аҳамияти катта эканлиги маълум бўлди. Европа Иттифоқи ва АҚШ амалиётида рақамли далиллар билан ишлашнинг аниқ стандартлари, махсус кибер полиция бўлинмалари ва замонавий криминалистика усуллари самарали қўлланилмоқда. Ўзбекистон учун ҳам ушбу тажрибани миллий қонунчиликка мос ҳолда татбиқ этиш мақсадга мувофиқдир.

Умуман олганда, тадқиқот натижалари шуни кўрсатадики, кибержиноятларга қарши курашиш тизимини такомиллаштиришда қуйидаги йўналишлар устувор аҳамиятга эга: амалдаги жиноят қонунчилигини замонавий киберҳавфларга мослаштириш, янги турдаги кибержиноятлар учун алоҳида ҳуқуқий нормаларни жорий этиш, рақамли далиллар билан ишлашнинг ягона стандартларини ишлаб чиқиш, шунингдек, ҳуқуқни муҳофаза қилувчи органларнинг техник ва кадрлар салоҳиятини ошириш.

Хулоса қилиб айтганда, кибержиноятлар глобаллашув шароитида барқарор ривожланиб бораётган мураккаб ҳуқуқий муаммолардан бири бўлиб қолмоқда. Уларнинг олдини олиш ва самарали ҳуқуқий тартибга солиш учун доимий равишда қонунчиликни такомиллаштириш, илмий тадқиқотларни кенгайтириш ва халқаро ҳамкорликни мустаҳкамлаш зарур. Бу эса, ўз навбатида, рақамли жамиятда шахс, жамият ва давлат хавфсизлигини таъминлашга хизмат қилади.

Фойдаланилган адабиётлар:

1. Ўзбекистон Республикаси Жиноят кодекси. – Т.: Адлия вазирлиги, 2025. – Lex.uz ҳуқуқий ахборот портали.
2. Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида”ги Қонуни. – 2022 йил. – Lex.uz.
3. Council of Europe. Convention on Cybercrime (Budapest Convention). – Budapest, 2001.
4. UNODC (United Nations Office on Drugs and Crime). Digital Evidence and Cybercrime Investigation Manual. – Vienna, 2022.
5. Mirziyodov A., Xolmo‘minov A. Jinoyat huquqi (Maxsus qism). – T.: Yuridik adabiyotlar nashriyoti, 2023.