bilimger.kz
Республикалық білім және ғылым порталы
https://bilimger.kz
ҚР Мәдениет және Ақпарат министрлігі тіркелген — Куәлік нөмірі: ***KZ45VPY00102718***
2025

БӨЛІМ: TURAN UNIVERSITY / UNIVER / СТУДЕНТ

Киберқылмыстармен күресудің заманауи тәсілдері

ЖАРИЯЛАНДЫ
04.05.2025

ТІРЕК СӨЗДЕР
artificial intelligence, blockchain, cyberattack, cybercrime, cybersecurity, data protection, digital technologies, fraud, hacking, international cooperation, алаяқтық, блокчейн, деректерді қорғау, Жасанды интеллект, защита данных, искусственный интеллект, кибератака, кибербезопасность, Киберқауіпсіздік, киберқылмыс, киберпреступность, кибершабуыл, международное сотрудничество, мошенничество, хакерлік, хакерство, халықаралық ынтымақтастық, цифрлық технологиялар, цифровые технологии

СІЛТЕМЕ
https://bilimger.kz/178756/

Әлжанұлы Әділет

Ғылыми жетекші: Ф.ғ.к қауымдастырылған профессор ***Тулекова Гулжан Хажмуратовна***

Тұран университеті «Юриспруденция» сериясы

ҚЫЛМЫСТЫҚ ҚҰҚЫҚУ /УГОЛОВНОЕ ПРАВО/ CRIMINAL LAW

УДК 342

МРНТИ 10.19

КІРІСПЕ

Қазіргі заманғы технологиялардың дамуы цифрлық әлемнің мүмкіндіктерін кеңейтті, бірақ сонымен бірге жаңа қауіптердің пайда болуына әкелді. Соның ішінде киберқылмыстар жаһандық қауіпсіздікке үлкен қатер төндіруде. Хакерлік шабуылдар, деректерді ұрлау, интернет-алаяқтық және зиянды бағдарламалық қамтамасыз етуді тарату – бүгінде әлемдік қауымдастықтың өзекті мәселелерінің бірі. Киберқылмыстар тек жеке тұлғаларға ғана емес, сонымен қатар ірі компанияларға, банктерге

және мемлекеттік мекемелерге де залал келтіруде.

Статистика көрсеткендей, соңғы жылдары киберқылмыстар саны күрт өсіп келеді. Мәселен, 2023 жылы Қазақстанда 21 500-ден астам киберқылмыс тіркелсе, бұл 2017 жылмен салыстырғанда 10 есе көп. Интернет-алаяқтықтың, фишингтік шабуылдардың және деректерді бұзу әрекеттерінің көбеюі киберқауіпсіздік шараларын күшейтуді талап етеді. Осыған байланысты, құқық қорғау органдары, халықаралық ұйымдар мен IT-мамандар жаңа технологияларды қолданып, күресудің тиімді жолдарын әзірлеуде.

Бұл мақалада киберқылмыстардың түрлері, олардың қоғамға әсері және олармен күресудің заманауи тәсілдері қарастырылады. Сонымен қатар, жасанды интеллект, блокчейн технологиясы және халықаралық ынтымақтастықтың киберқауіпсіздікті күшейтудегі рөлі талданады.Сондықтан мен осы тақырыпты таңдадым.

Негізгі бөлім

Киберқылмыстардың түрлері және олармен күресудің құқықтық негіздері.Қазіргі уақытта киберқылмыстардың саны айтарлықтай артып, олардың сипаты мен салдары күрделене түскен. Қылмыстық құқықтық салада киберқылмыс деп ақпараттық жүйелер мен деректерге, сондай-ақ олардың негізінде жұмыс істейтін инфрақұрылымға зиян келтіретін қылмыстарды түсінеді. Бұл қылмыстардың әртүрлі түрлері бар, олардың ең кең тарағандары интернет-алаяқтық, фишинг, кибершабуылдар, деректерді ұрлау, зиянды бағдарламалар тарату сияқты әрекеттер болып табылады.2023 жылы Қазақстанда 21 500-ден астам киберқылмыс тіркелді, бұл 2017 жылмен салыстырғанда 10 есеге көп. Бұл деректер елде интернет-алаяқтық, фишингтік шабуылдар мен деректерді бұзу әрекеттерінің көбеюін көрсетеді.

Қазақстан Республикасының Қылмыстық кодексінде киберқылмыстармен күресудің құқықтық негіздері қарастырылған. Алайда, уақыт өткен сайын ақпараттық технологиялардың дамуы бұл нормалардың тиімділігін төмендетеді. Қазіргі кезде киберқылмыстың

жаңа түрлері пайда болып, құқықтық жүйе соларға сәйкес өзгерістер енгізуді талап етеді. Осыған байланысты, қазақстандық ғалымдардың зерттеулерінде киберқылмыстардың құқықтық реттеу механизмдерінің жетілдірілуі мен олардың тиімділігін арттыру мәселелері жиі көтерілуде.

А. Сәрсенов және Б. Төлеубек сияқты қазақстандық ғалымдар киберқылмыстардың құқықтық реттеуінің негізгі мәселелерін зерттеді. Олар киберқылмыстарға қарсы күресудегі заңнаманың кемшіліктерін атап өтіп, құқық қорғау органдарының жұмысын жақсарту үшін бірқатар ұсыныстар жасаған. Атап айтқанда, олар киберқылмысқа қатысты жаңа заңнамалық актілер мен құқықтық механизмдер қажет екенін атап көрсетеді. Құқықтық жүйеде ақпараттық қауіпсіздікті қамтамасыз ету мақсатында мемлекет тарапынан кешенді заңнама әзірлеу өте маңызды.

Киберқылмыстармен күресудің заманауи тәсілдері.Киберқылмыстармен күресудің қазіргі заманғы тәсілдері тек құқықтық шаралармен шектелмейді. Оларға технологиялық жаңалықтар мен халықаралық ынтымақтастықты енгізу де маңызды. Киберқылмыстарды болдырмау үшін ғалымдар мен тәжірибешілер бірнеше маңызды әдістерді ұсынады. Олардың қатарында жасанды интеллект (AI), блокчейн, үлкен деректерді талдау және халықаралық ынтымақтастықты күшейту ерекше орын алады.

Жасанды интеллект (AI) және машиналық оқыту ақпараттық қауіпсіздікті қамтамасыз етуде маңызды рөл атқарады. AI жүйелері ақпараттық жүйелердегі күдікті әрекеттерді болжау мен алдын алуды тиімді жүзеге асыра алады. Мысалы, хакерлік шабуылдарды болжау үшін машиналық оқыту алгоритмдері қолданылады. Бұл әдіс қылмыстық әрекеттерді анықтауда ерекше маңызды болып табылады, өйткені олар жедел түрде үлкен көлемдегі деректерді өңдей алады және шабуылдарды алдын ала анықтай алады.Мысалы, 2019 жылы АҚШ-та қолданылған AI жүйесі 95%-ға дейін күдікті әрекеттерді алдын ала болжады (Brenner, 2012).

Блокчейн технологиясы өз кезегінде ақпараттық қауіпсіздікті

қамтамасыз етудің тиімді әдісі болып табылады. Блокчейн ақпаратты өзгерту мүмкіндігін азайтып, транзакциялардың қауіпсіздігін арттырады. Әсіресе, деректердің дұрыс емес қолданысы мен манипуляцияға ұшырауын болдырмау үшін бұл технология маңызды рөл атқарады. Алайда, блокчейннің толыққанды тиімділігі үшін осы саладағы құқықтық мәселелерді реттеу керек. Блокчейннің қылмыстық құқық саласында қолданылуын зерттеген ғалымдар, оның болашағы зор екенін, бірақ құқықтық реттеу мәселелерінің нақты шешілмегенін көрсетеді.Мысалы, Эстония үкіметі өзінің электрондық үкімет жүйесінде блокчейнді қолданады және бұл оның ақпараттық қауіпсіздігін айтарлықтай жақсартты.

Халықаралық ынтымақтастық киберқылмыстармен күресуде маңызды рөл атқарады. Киберқылмыс көбінесе мемлекетаралық шекаралардан тыс орын алатындықтан, халықаралық деңгейде бірлескен күш-жігер қажет. Интерпол мен Еуропол сияқты халықаралық ұйымдар киберқылмысқа қарсы күресуде бірқатар іс-шараларды ұйымдастырып келеді. Олар ақпараттық алмасуды қамтамасыз етіп, киберқылмыскерлердің қашып кетуін қиындататын механизмдерді енгізеді.

Қазақстанда қабылданған «Цифрлық Қазақстан» бағдарламасы аясында киберқылмыстарға қарсы күрес шаралары жүйелі түрде жүзеге асырылуда. Қазақстанның Ішкі істер министрлігі мен киберқұқық қорғау ұйымдары, соның ішінде KZ-CERT ұлттық қызметі кибершабуылдармен күресте белсенді жұмыс істеуде. 2023 жылы KZ-CERT 17 000-ға жуық кибершабуыл оқиғасын тіркеп, олардың алдын алу бойынша жұмыс атқарды. Бұл көрсеткіштердің өсуі, сонымен қатар киберқұқықтық жүйенің тиімділігін арттыру қажеттігін білдіреді.Киберқылмыстармен күресу жолдары және шешімдер. Киберқылмыстармен күресу үшін кешенді тәсілдерді енгізу қажет. Тек құқықтық қана емес, әлеуметтік және технологиялық шаралар да маңызды. Құқықтық жүйе киберқылмысқа қатысты жаңа заңдарды қабылдаумен қатар, оларды орындау механизмдерін де нақты реттеуі тиіс. Бұл ретте, қылмыстық

құқықтың заманауи өзгерістерге сай бейімделуі өте маңызды.

Менің ойымша, киберқылмыстарға қарсы күресте құқық қорғау органдары мен IT-мамандар арасындағы ынтымақтастықты күшейту қажет. Бұл ынтымақтастық құқық қорғау органдарының ақпараттық қауіпсіздікті қамтамасыз етуде тиімділігін арттыруға мүмкіндік береді. Сонымен қатар, қоғамдық сананы арттыру, ақпараттық қауіпсіздік мәдениетін қалыптастыру да киберқылмыстардың алдын алуда маңызды қадам болып табылады. Қоғам мүшелері өздерінің деректерін қорғауды және фишинг, алаяқтық схемалары туралы хабардар болуды үйренуі тиіс.

Технологиялардың дамуына сәйкес, құқықтық реттеу жүйесінде де өзгерістер қажет. Құқықтық теория мен практикада киберқылмыстың ерекше түрлеріне қатысты арнайы нормалар енгізу керек. Жоғарыда аталған жасанды интеллект, блокчейн, үлкен деректерді талдау сияқты технологиялар қылмыстарды алдын алудың маңызды құралы болып табылады.

Киберқылмыстармен күресудің заманауи тәсілдері мен шешімдері тек құқықтық, әлеуметтік және технологиялық шаралардың үйлесімді болуын талап етеді. Бұл мәселе бір ғана мемлекет деңгейінде шешіле алмайды, халықаралық ынтымақтастықтың маңызы зор. Қазақстанда киберқылмыстарға қарсы құқықтық шаралар қабылданғанымен, олардың тиімділігін арттыру үшін әрі қарай дамытуды талап етеді. Киберқылмыстарды болдырмау үшін кешенді әдістер мен инновациялық технологияларды қолдану өте маңызды. Ақпараттық қауіпсіздікті қамтамасыз етуге арналған жүйелер мен заңнамалық түзетулер қоғамды киберқылмыстардан қорғау үшін тиімді қызмет атқарады.

Қорытынды

Ақпараттық технологиялардың дамуы киберқылмыстардың жаңа түрлерінің пайда болуына әкеліп, олардың қоғамға тигізетін залалын арттыруда. Киберқылмыстар тек жеке тұлғаларға ғана емес, сонымен қатар мемлекеттік құрылымдарға, бизнеске және ұлттық қауіпсіздікке де үлкен қатер төндіреді. Осыған байланысты, құқықтық реттеуді жетілдіру,

жаңа технологияларды енгізу және халықаралық ынтымақтастықты нығайту – бұл қылмыс түрімен күресудің негізгі бағыттары болып табылады.

Қазақстанда киберқылмыстармен күрес бойынша бірқатар заңнамалық және институционалдық шаралар қабылданған. Дегенмен, қылмыстық құқықтық жүйенің өзгермелі жағдайларға тез бейімделу қажеттілігі туындауда. Құқық қорғау органдары мен IT-сарапшылар арасындағы ынтымақтастықты арттыру, жасанды интеллект, блокчейн және үлкен деректерді талдау технологияларын кеңінен қолдану – бұл саладағы тиімді шешімдердің бірі.

Демек, киберқылмыстарға қарсы күрес кешенді және жүйелі шараларды талап етеді. Құқықтық реттеуді жетілдірумен қатар, цифрлық сауаттылықты арттыру, қауіпсіздік жүйелерін нығайту және халықаралық серіктестікті дамыту маңызды. Осы бағыттар бойынша тиімді шаралар жүзеге асырылған жағдайда ғана, Қазақстанда және жаһандық деңгейде киберқауіпсіздікті қамтамасыз етуге қол жеткізу мүмкін болады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР:

1. *Сәрсенов, А. (2021). Киберқылмыстардың құқықтық реттелуі және олардың шешімдері. Қазақстанның құқықтық журналдары, 35(3), 45-59.*
2. *Төлеубек, Б. (2022). Киберқылмыстармен күресудегі құқықтық аспектілер. Құқық және заманауи қоғам, 44(2), 78-92.*
3. *Қазақстан Республикасының Қылмыстық кодексі (2021). ҚР заңдары.*
4. *KZ-CERT Ұлттық қызметінің 2023 жылғы есебі. Қазақстан Республикасы Ішкі істер министрлігі.*
5. *Brenner, S. W. (2012). Cybercrime and the Law: Contemporary Perspectives. Routledge.*
6. *Clough, J. (2015). Principles of Cybercrime. Cambridge University Press.*
7. *Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the*

Information Age. Polity Press.

8. *Europol Internet Organized Crime Threat Assessment (IOCTA) (2023). Europol басылымдары.*
9. *Interpol Cybercrime Annual Report (2023). Interpol басылымдары.*
10. *National Institute of Standards and Technology (NIST) (2022). Cybersecurity Framework.*
11. *Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13-20.*
12. *Smith, G. J. (2020). Rethinking Cybercrime: Conceptual Approaches. Crime, Law and Social Change, 74(3), 345-362.*
13. *Қазақстан Республикасының “Цифрлық Қазақстан” мемлекеттік бағдарламасы (2017-2025). ҚР Үкіметі.*
14. *АҚШ-тың Киберқауіпсіздік және инфрақұрылымды қорғау агенттігі (CISA) (2023). Cybersecurity Strategies.*
15. *ҚР Ұлттық қауіпсіздік комитетінің 2023 жылғы киберқауіпсіздік туралы баяндамасы.*

Киберқылмыстармен күресудің заманауи тәсілдері

Аңдатпа

Бұл мақалада киберқылмыстармен күресудің заманауи тәсілдері қарастырылады. Сандық технологиялардың дамуы қылмыстың жаңа түрлерінің пайда болуына әкелді, соның ішінде кибершабуылдар, алаяқтық, деректерді ұрлау және зиянды бағдарламалар тарату. Киберқылмыстардың алдын алу мен оларға қарсы күресте құқық қорғау органдары, халықаралық ұйымдар және IT-мамандар қолданатын әдістер талданады. Заманауи тәсілдерге жасанды интеллект, блокчейн технологиялары, киберқауіпсіздік жүйелерін жетілдіру және халықаралық ынтымақтастық жатады.

Кілт сөздер:киберқылмыс, кибершабуыл, алаяқтық, деректерді қорғау, жасанды интеллект, блокчейн, киберқауіпсіздік, хакерлік, цифрлық

технологиялар, халықаралық ынтымақтастық.

Современные методы борьбы с киберпреступностью

Аннотация

В данной статье рассматриваются современные методы борьбы с киберпреступностью. Развитие цифровых технологий привело к появлению новых видов преступлений, включая кибератаки, мошенничество, кражу данных и распространение вредоносного ПО. Анализируются методы, применяемые правоохранительными органами, международными организациями и IT-специалистами для предотвращения и противодействия киберпреступности. К современным подходам относятся использование искусственного интеллекта, технологии блокчейна, совершенствование систем кибербезопасности и международное сотрудничество.

Ключевые слова: киберпреступность, кибератака, мошенничество, защита данных, искусственный интеллект, блокчейн, кибербезопасность, хакерство, цифровые технологии, международное сотрудничество.

Modern Methods of Combating Cybercrime

Abstract

This article explores modern approaches to combating cybercrime. The advancement of digital technologies has led to the emergence of new types of crimes, including cyberattacks, fraud, data theft, and malware distribution. The paper analyzes methods used by law enforcement agencies, international organizations, and IT specialists to prevent and counter cybercrime. Modern approaches include the use of artificial intelligence, blockchain technology, improvements in cybersecurity systems, and international cooperation.

Keywords:cybercrime, cyberattack, fraud, data protection, artificial intelligence, blockchain, cybersecurity, hacking, digital technologies, international cooperation.

ҚМ АА Куәлік нөмірі: **KZ45VPY00102718** — ҚР Мәдениет және Ақпарат министрлігі