ОШ МАМЛЕКЕТТИК УНИВЕРСИТЕТИНИН ЖАРЧЫСЫ. УКУК

ВЕСТНИК ОШСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА. ПРАВО

JOURNAL OF OSH STATE UNIVERSITY. LAW

e-ISSN: 1694-8661
№1(6)2025, 169-175

УДК:
DOI: 10.52754/16948661_2025_1(6)_26

ЖАСАЛМА ИНТЕЛЛЕКТИ КОЛДОНУУ АРКЫЛУУ ЖҮРГҮЗҮЛГӨН КИБЕРКЫЛМЫШТУУЛУКА КАРШЫ КҮРӨШҮҮНҮН ТЕОРИЯЛЫК АСПЕКТИЛЕРИ

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

THEORETICAL ASPECTS OF FIGHTING CYBERCRIME USING ARTIFICIAL INTELLIGENCE

Токтомамбетова Кыял Кубанычбековна
Токтомамбетова Кыял Кубанычбековна
Toktomambetova Kiyal Kubanychbekovna

ю.и.к., улук окутуучу, Ош мамлекеттик университети
к.ю.н., старший преподаватель, Ошский государственный университет
Candidate of Law Science. Senior lecturer, Osh State University

---

Маматазизова Эльмира Кубаничбековна
Маматазизова Эльмира Кубаничбековна
Mamatazizova Elmira Kubanichbekovna

ю.и.к., доцент, Ош мамлекеттик университети
к.ю.н., доцент, Ошский государственный университет
Candidate of Law Science. Associate Professor, Osh State University

---

Эркебаев Сагынбек Сейдалиевич
Эркебаев Сагынбек Сейдалиевич
Erkebaev Sagynbek Seidalievich

магистрант, Ош мамлекеттик университети
магистрант, Ошский государственный университет
Master's student , Osh State University

ЖАСАЛМА ИНТЕЛЛЕКТИ КОЛДОНУУ АРКЫЛУУ ЖҮРГҮЗҮЛГӨН КИБЕРКЫЛМЫШТУУЛУКА КАРШЫ КҮРӨШҮҮНҮН ТЕОРИЯЛЫК АСПЕКТИЛЕРИ

Аннотация

Маанилүүлүк. Макалада жасалма интеллект технологияларын колдонуу аркылуу жасалган кибер кылмыштуулук жөнүндө жазылган. Санариптик технологиянын өнүгүүсүнүн натыйжасында кибер кылмыштуулуктун динамикасынын жогорулагандыгы жөнүндө айтылат. Кибер кылмыштуулуктун түрлөрүнө аныктама берилет. Кыргыз Республиксынын Кылмыш-жаза кодексинде каралган кибер коопсуздукка каршы кылмыштарга карата жоопкерчиликтерге талдоо жүргүзүлөт. Кибер кылмыштуулуктун субъектилери мамлекеттик кызматчылардын атын жамынып алып эң жеңил жолдор менен эле алдамчылык аракеттерин жасагандыгына укуктук талдоо жүргүзүлөт. Кибер кылмыштуулук боюнча 2024-2025 жылдарга статистикалык маалымат берилген. Кибер кылмыштуулукка каршы туруу үчүн актуалдуу сунуштар берилди.

Ачкыч сөздөр: санариптик кодекс, санариптик сабаттуулук, санариптик технология, жасалма интеллект, кибер кылмыштуулук, кибер алдамчылык, кибер чабуулу

Теоретические аспекты борьбы с киберпреступностью с использованием искусственного интеллекта

Аннотация

Актуальность. В статье рассматриваются киберпреступления, совершаемые с использованием технологий искусственного интеллекта. Сообщается, что динамика киберпреступности возросла в результате развития цифровых технологий. Определены виды киберпреступности. Будет проведен анализ ответственности за преступления против кибербезопасности, предусмотренной Уголовным кодексом КР. Проводится правовой анализ, чтобы определить, как киберпреступники выдают себя за государственных служащих и совершают мошеннические действия наиболее простыми способами. Приведена статистическая информация о киберпреступности за 2024-2025 годы. Даны соответствующие рекомендации по борьбе с киберпреступностью.

Ключевые слова: цифровой кодекс, цифровая грамотность, цифровая технология, искусственный интеллект, киберпреступность, кибермошенничество, кибератака

Theoretical aspects of fighting cybercrime using artificial intelligence

Abstract

Relevance. The article discusses cybercrimes committed using artificial intelligence technologies. It is reported that the dynamics of cybercrime has increased as a result of the development of digital technologies. The types of cybercrime are defined. An analysis of liability for crimes against cybersecurity provided for by the Criminal Code of the Kyrgyz Republic will be conducted. A legal analysis is carried out to determine how cybercriminals impersonate government officials and commit fraudulent actions in the simplest ways. Statistical information on cybercrime for 2024-2025 is provided. Relevant recommendations for combating cybercrime are given.
.

Keywords: digital code, digital literacy, digital technology, artificial intelligence, cybercrime, cyber fraud, cyber attack

Киришүү

Актуалдуулугу. Азыркы дүйнөдө жасалма интеллект (AI) өтө тездик менен өнүгүп, жашообуздун бардык тармагына, т.а. медицина менен билим берүүдөн тартып, өнөр жай жана каржы секторуна чейинки ар кандай тармактарга сүңгүп кирүү аркылуу адамзаттын жумушуна олуттуу артыкчылыктарды сунуштап келүүдө. Бирок, бул позитивдүү тенденциялар менен катар эле, жасалма интелектти зыяндуу максаттарда, айрыкча киберкылмыштуулукта колдонуу мүмкүндүгү жөнүндө кооптонуулар да күчөп бараткандыгы көпчүлүккө маалым боло баштады.

Бул макала Кыргыз Республикасында жасалма интеллект технологияларын колдонуу аркылуу жасалып жаткан киберкылмыштуулук феноменин изилдөөгө арналган. **Макаланын темасынын актуалдуулугу** жасалма интеллекттин мүмкүнчүлүктөрүнүн экспоненциалдуу өсүшүнө жана натыйжада киберкоркунучтардын жаңы, кыйла татаал жана аныктоо бир кыйла кыйын болчуу түрлөрүнүн пайда болушуна байланыштуу. Мындай кылмыштарды жасоонун механизмдерин жана ыкмаларын түшүнүү, ошондой эле Кыргызстан үчүн мүмкүн болуучу кесепеттерге талдоо жүргүзүү келечекте киберкоопсуздукка каршы туруу жана камсыздоо боюнча эффективдүү стратегияларды иштеп чыгуунун ачкычы болуп саналат.

Санариптик технологиялардын өнүгүүсүнүн азыркы этабында кибер кылмыштуулукка, кибер алдамчылыкка каршы тез жана натыйжалуу күрөшүү ар бир мамлекет үчүн башкы приритеттүү багыттардан болуп саналат.

Кыргызстандагы кибермейкиндикти коргоо стратегиясында[2] адамдардын жашоосунда чындап эле алардын ажырагыс бөлүгү болуп калган маалыматтык системалардын маанилүүлүгү жана зарылчылыгы туура белгиленген. Бул санариптик чөйрөдө жарандардын, бизнестин жана мамлекеттин коопсуздугун камсыз кылуу үчүн бул системаларды коргоо жана кибер коркунучтарга каршы күрөшүү маанилүү экенин баса белгилейт.

Санариптик технологияларды өнүктүрүү эбегейсиз пайда алып келет, бирок ошол эле учурда кибер кылмыштуулук менен байланышкан жаңы тобокелдиктерди жаралууда. Ошондуктан, кибер алдамчылыктын алдын алуу, аныктоо жана бөгөт коюу боюнча активдүү жана координацияланган иш ийгиликтүү санариптик трансформациянын ажырагыс бөлүгү болуп саналат.

"Кибер алдамчылык" жана "кибер кылмыш" терминдеринин пайда болуусу Америкада 1960-жылдары компьютерлештирүүнүн алгачкы баскычтарына туура келет. Ошол эле учурда компьютердик технологияларды колдонуу менен жасалган алгачкы кылмыштар да каттала баштаган.

Белгилей кетчү нерсе, бул алгачкы киберкылмыштардын табияты азыркыдан башкача болгон, анткени компьютердик системалар азыркыга салыштырмалуу азыраак таралган жана башка функцияларга ээ болгон. Бирок, ошондо да кылмышкерлер жаңы технологияларды кылмыштуу максатта колдонуунун жолдорун издеп жатышкан.

1990-жылдар илгерилеген сайын, Интернеттин жайылышы жана өнүгүшү менен интернет-алдамчылыктын олуттуу өсүшү байкалган. Байланыш, соода жана маалымат алмашуу үчүн жаңы мүмкүнчүлүктөрдүн пайда болушу киберкылмышкерлер пайдалана баштаган жаңы чабалсыздыктарды да жаратты. Бул интернет-алдамчылыктын ар кандай түрлөрүнүн пайда болушуна жана өнүгүшүнө алып келди, алар бүгүнкү күндө дагы актуалдуу бойдон калууда.

Кибер алдамчылык - бул заманбап маалыматтык технологияларды колдонуу аркылу жасалган, бирок ошол эле учурда мыйзам тарабынан тыюу салынган ар кандай иштер. Анын максаты башка бирөөнүн мүлкүн, анын ичинде жарандардын жеке маалыматтарын жана финансылык ресурстарын мыйзамсыз тартып алуу болуп саналат. Башкача айтканда, компьютерлердин, компьютердик программалардын же тармактардын иштөөсүнө уруксатсыз кирүү, ошондой эле компьютердик маалыматтарды мыйзамсыз өзгөртүү же Интернет аркылуу башка бирөөнүн мүлкүн уурдоого багытталган мыйзамсыз аракет.

Кибер алдамчылыктын негизги төмөнкүдөй түрлөрү бар:

1) Маалыматтарды бузуп, чогултуучу, көчүрүүчү жана кээде жок кылган түрдүү вирустардын киришине байланышкан кылмыштарды камтыган *зыяндуу программалык камсыздоо*;

2) *Форд*, бул жасалма, зыяндуу веб-сайтта сатып алуу жасаган кардардын банктык картасынан жеке маалыматтарды уурдоо;

3) *Ортомчулар (MitM) аркылуу жасалган киберчабуудар*, бул сүйлөшүп жаткан учурда, мисалы: электрондук кат алышуу сыяктуу байланыш учурунда үчүнчү тарап сүйлөшүүгө кошулуп, жашыруун маалыматты кармап, сактап, сыртка чыгарып кетишин билдирет;

4) *Фишинг.* Кардардын жеке маалыматтарын, мисалы, банктык эсептердин логиндерин жана ачкыч сөздөрүн (паролдорун) уурдоо, көбүнчө жасалма веб-сайттарга шилтемелер менен электрондук почталарды колдонуу аркылуу ишке ашырылат;

5) *Күн көрө элек алсыздыктар* (орусча: уязвимости «нулевого дня»). Бул жаңы эле пайда болгон, бирок чабал жерлери бар программалык камсыздоолор аркылуу ишке ашырылат. Ал чабал жактар иштеп чыгуучулар тарабынан али аныктала жана корголо элек болот;

6) *Нигериялык каттар.* Электрондук почта аркылуу таркатылып, юридикалык кызматтарды төлөө үчүн акча которуу өтүнүчү менен мурас жөнүндө маалыматты камтыган билдирүүлөр;

7) *Онлайн капчыктар аркылуу жасалчуу алдамчылык.* Товарды онлайн сатып алууда кардар тийиштүү төлөмдү которот, бирок кайра акчадан да, товардан да жок отуруп калышат;

8) *DDoS-чабуулу "Кызмат көрсөтүүдөн баш тартмай".* Алар бир эле учурда бир нече жалган сурамалыктарды (запрос) кароо учурунда көрүнөт, алар жүктөмдүн чоңдугуна байланыштуу ресурсту өчүрөт;

9) *DNS серверине болгон чабуул.* Бул домендер, түзүлүштөрдүн IP даректери жана почтанын маршруттары жөнүндө маалыматты алууга багытталган киберчабуул.

Кибералдамчылыктын аталган түрлөрүнө, айрым авторлор электрондук төлөм каражаттарынын чөйрөсүндө жасалган кылмыштарды да кошуу зарылдыгын сунушташууда.

Албетте, Кыргыз Республикасынын мамлекеттик саясаты да жөн турган жери жок. Азыркы этапта киберкылмыштарды иликтөө Ички иштер министрлигинин 10-башкармалыгынын, тактап айтканда, Кибертеррористикке каршы күрөшүү башкармалыгынын компетенциясына кирет. КР Кылмыш-жаза кодексине “Киберкоопсуздукка каршы кылмыштар” деген өзүнчө 40-глава киргизилген, анын 4-беренесинде төмөнкүлөр каралган:

- 319-берене. Компьютердик маалыматтарга жана электрондук документтерге, маалыматтык системага же электр байланыш тармагына уруксатсыз жетүү
- 320-берене. Зыяндуу программалык продуктуларды түзүү
- 321-берене. Кибер-саботаж
- 322-берене. Электрондук билдирүүлөрдү массалык түрдө жайылтуу

Кыргыз Республикасынын 2021-жылдын 28-октябрындагы № 127 Кылмыш-жаза кодексине жана 2021-жылдын 28-октябрындагы № 128 Укук бузуулар жөнүндө кодексине ылайык жеке маалыматтарды коргоо жөнүндө Кыргыз Республикасынын мыйзамдарын бузгандык үчүн жоопкерчилик киргизилген. Аталган жоопкерчилик боюнча киберкылмышардын статистикасына карай турган болсок, анда электрондук төлөм каражаттарына байланыштуу кылмыштар көптөгөн кооптонууларды жаратат. Мисалы, https://www.tazabek.kg/ сайтынын маалыматтарына ылайык, 2024-жылы Кыргызстан боюнча 1 миң 658 кылмыш катталган. Анын көпчүлүгү Бишкек шаарына тиешелүү[3]. Мындан сырткары, Кыргызстан 470 миң долларлык банк эсеби менен алдамчылыкка шектелген аял жаранды Казакстанга үстүбүздөгү жылдын апрель айында өткөрүп берген. https://www.turmush.kg/ сайтынын малыматы боюнча, 2025-жылдын бүгүнкү күнүнө чейин Жалал-Абад облусу боюнча кибер алдамчылыктын 32 учуру катталган[4].

Жыл өткөн сайын алдамчылык иштер татаалдашып, кылмышкерлер уурдоонун жаңы ыкмаларын ойлоп табууда. Адам факторунан сырткары, учурда жасалма интелекттин (нейроторчолордун) мүмкүнчүлүктөрүнөн пайдалана башташты. Хакерлер алдоо жана опузалап акча алуу максатында генерацияланган үн, видео жана сүрөттөрдү активдүү колдоно башташкан. Мисалы, КР Президенти Садыр Жапаров ж.б. өлкө жетекчилигинин видеолору нейрондук түйүндөр тарабынан иштелип чыгып, кийин социалдык тармактарга оңой-олток акча табууга чакырык катары жарыяланып да жатат[5].

Эл аралык McAfee киберкоопсуздук компаниясынын сурамжылоосуна ылайык, респонденттердин 25% 2023-жылы жасалма интелекттин үн-алдамчылыгына туш болушкан. Мындан тышкары, бул топтун 77% генерацияланган үн-алдамчылыкка каражаттарын алдырып жиберишкен[6].

Жасалма интелекттин натыйжасында “фишинг” деп аталган кибер алдамчылык жаңы деңгээлге чыгууда. “Газинформсервис” киберкоопсуздук борборунун маалыматы боюнча, чабуулдардын санынын жылдык өсүшү 20-25% түзөт. Эгерде өз алдынча иштеген алдамчы күнүнө 300гө чейин фишинг коңгуроолорду-чалууларын жасай алса, ЖИ-н жардамы менен бул сан 40-50 миңге чейин көбөйүшү мүмкүн.

Социалдык тармактардагы жалпыга жеткиликтүү маалыматты талдоо менен алар мүмкүн болгон жабырлануучулардын баарлашуу стилин жана кызыкчылыктарын кылдат изилдешет. Андан кийин, табигый тилди иштетүү алгоритмдерин колдонуп, Жасалма интеллект достор, кесиптештер, жетекчилер, атүгүл мамлекеттик органдар менен чыныгы кат алышуудан стили боюнча айырмалоо дээрлик мүмкүн болбогон, о.э. өтө ынанымдуу фишинг билдирүүлөрүн жаратышууда.

Мисал катары, чабуулчулар Кыргыз Республикасынын Мамлекеттик салык кызматынын атын жамынып, салыктарды онлайн режиминде төлөөнү сунушташууда же Улуттук банктын атынан купуялуулукту текшерүү процедурасынан өтүүнү сунуштаган электрондук каттарды жөнөтүшүүдө. Жыйынтыгында жаңылышкан колдонуучулар өздөрүнүн жеке маалыматтарын жана акча каражаттарын мамлекеттик органдарга өткөрүп

берип жатышат деп ойлошкону менен, чындыгында бул маалымат алдамчылардын колуна түшүп жаткан болууда.

Жасалма интелект менен иштеген кибер алдамчылык коркунучу азыр жөнөкөй тексттик билдирүүлөрдөн алда канча ашып кетти, анткени ЖИ жасалма видео жана аудио жазуулар болгон өтө реалдуу терең дипфейктерди түзүүгө жөндөмдүү экен. Бул шылуундар жабырлануучуну акча которуу, сырсөздөрдү же башка купуя маалыматты ачыкка чыгаруу сыяктуу кооптуу аракеттерди жасоого көндүрүү үчүн тааныш адамдын үнүн жана сырткы көрүнүшүн колдонушууда. Мындай алдамчылыкты байкап калуу өтө татаал маселе жана алдамчылар уламдан-улам татаалданган, кээде абсурддуу ыкмаларды, анын ичинде өлгөн жакындарынын акчалай жардам сурап телефон чалуусун имитациялоону колдонушууда. Мисалы, 2024-жылдын башында, башкы кеңсеси Кытайда жайгашкан глобалдык каржылык кызмат көрсөтүүчү компаниянын кызматкери дипфейктин курмандыгы болуп калган. Мында чабуулчулар видеоконференция учурунда компаниянын каржы директору жана башка жетекчилеринин кейпин кийип, кызматкерге 25 миллион долларлык “жашыруун транзакцияны” өткөрүп беришине чейин жетишишкен, анткени жасалма интелект жандуу конференция катарында берки кызматкер менен сүйлөшүп, акча которууга чейин ынандыра алган.

Корутунду

Заманбап санариптик технологияларды өнүктүрүү контекстинде кибер алдамчылык көйгөйүнө жүргүзүлгөн талдоо бир катар маанилүү тыянактарды чыгарууга мүмкүндүк берет. Кеңири жайылган санариптештирүү шартында, маалыматтык системалар жарандардын күнүмдүк турмушуна жана уюмдардын ишмердүүлүгүнө терең интеграцияланган учурда, санариптик чөйрөдө коопсуздукту, туруктуулукту жана ишенимди камсыз кылуу үчүн киберкылмыштуулукка, өзгөчө кибералдамчылыкка каршы күрөшүү өзгөчө мааниге ээ экендиги айдан ачык. Тарыхый маалыматтар көрсөткөндөй, киберкылмыштуулуктун алгачкы көрүнүштөрү компьютерлештирүүнүн башталышында пайда болгон, бирок Интернеттин өнүгүшү жана маалыматтык технологиялардын татаалдашуусу менен кибер алдамчылыктын масштабы жана татаалдыгы бир нече эсеге өстү. Бүгүнкү күндө бул көп кырдуу көрүнүш жеке колдонуучуларга да, ири уюмдарга жана мамлекеттик органдарга да олуттуу коркунуч жаратууда.

Интернет-алдамчылыктын заманбап түрлөрүн талдоо чабуулчулардын тактикасынын жана куралдарынын тынымсыз эволюциясын көрсөтүп турат. Кесепеттүү программаларды жана фишингдик чабуулдарды жайылтуудан баштап, “күн көрө элек алсыздыктарды” жана онлайн капчык шылуундарына чейин киберкылмышкерлер өз ыкмаларын тынымсыз өнүктүрүшөт. Жасалма интеллект технологияларынын тез өнүгүшү өзгөчө тынчсызданууну жаратат, алар өтө жекелештирилген жана ынандырарлык чабуулдар үчүн жаңы, анын ичинде эң сергек колдонуучуларды да алдай ала турган реалдуу дипфейктерди түзүү сыяктуу мүмкүнчүлүктөрдү ачып жатат.

Бүткүл дүйнөдөгүдөй эле Кыргыз Республикасында да кибералдамчылыкка каршы жигердүү күрөшүү зарылчылыгы таанылган. Ички иштер министрлигинин алдында адистештирилген бөлүм түзүлүп, киберкоркунучтар тууралуу калктын жана уюмдардын маалымдуулугун жогорулатуу боюнча иш-чаралар жүргүзүлүүдө, кибермейкиндикти коргоо боюнча стратегиялар иштелип чыгып, ишке ашырылууда. Бирок, талдоо көрсөткөндөй, көйгөй актуалдуу бойдон калууда жана каршы чараларды мындан ары күчөтүүнү талап кылат.

Кибер алдамчылыкка каршы эффективдүү күрөш комплекстүү мамилени талап кылат, анын ичинде мыйзамдык базаны өркүндөтүү (КР Санариптик Кодексин батыраак кабыл алуу), маалыматтык системалардын техникалык коопсуздугун жогорулатуу, эл аралык кызматташтыкты активдештирүү, калктын санариптик сабаттуулугун тынымсыз жогорулатуу. Пайда болгон коркунучтарга ыкчам жооп берүү гана эмес, алдамчылыктын жаңы түрлөрүн, анын ичинде жасалма интеллектти колдонуу менен байланышкандарды алдын алуу жана алдын алуу менен алдыда иштөө зарыл.

Жыйынтыктап айтканда, динамикалуу өнүгүп жаткан санариптик дүйнөнүн шартында кибер алдамчылыкка каршы туруу үзгүлтүксүз процесс болуп санала тургандыгын, мамлекеттин, бизнестин жана бүтүндөй коомдун туруктуу көңүл буруусун, адаптациясын жана күч-аракеттерин бириктирүүнү талап кылаарын баса белгилей кетүү керек. Биргелешкен күч-аракеттер аркылуу гана биз жарандардын жана мамлекеттин жыргалчылыгы үчүн маалыматтык технологияларды андан ары өнүктүрүүгө көмөктөшүүчү коопсуз жана ишенимдүү санариптик чөйрөнү түзө алабыз.

Колдонулган булактар:

1. Кыргызской Республикасынын Кылмыш-жаза кодекси жалпы бөлүм, 2021-жылдын 28-октябры № 127, 2025-жылдын 14-мартындагы №56 өзгөртүү толуктоолору менен, [электронный ресурс] http://cbd.minjust.gov.kg/
2. Кыргызстандагы кибермейкиндикти коргоо стратегиясы. [Электрондук ресурс]. Кирүү режими: https://digital.gov.kg/ky/activities/strategiya-zashhity-kiberprostanstva-v-kyrgyzstane.
3. https://www.tazabek.kg/news:2262145/?from=tazabek&place=newsload.
4. https://www.turmush.kg/ru/news:2261908/
5. https://kg.akipress.org/news:2105057.
6. Как ИИ помогает кибермошенникам и противостоит им. Подробнее на РБК: кирүү режими: https://trends.rbc.ru/trends/industry/6756bcfb9a7947690bdc259a?from=copy.