ОШ МАМЛЕКЕТТИК УНИВЕРСИТЕТИНИН ЖАРЧЫСЫ

ВЕСТНИК ОШСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

BULLETIN OF OSH STATE UNIVERSITY

ISSN: 1694-7452 e-ISSN: 1694-8610

№2/2024, 479-494

ТЕХНИКА

УДК: 004.056.57

DOI: 10.52754/16948610_2024_2_47

ВИРТУАЛДЫК КЫЛМЫШ ПРОЦЕССТЕРИНДЕ САНАРИПТИК ИЗДЕРДИ АНЫКТОО: САНАРИПТИК КРИМИНАЛИСТИКАЛЫК ИЗИЛДӨӨЛӨРГӨ СЕРЕП САЛУУ

ОБНАРУЖЕНИЕ ЦИФРОВЫХ СЛЕДОВ В ВИРТУАЛЬНЫХ УГОЛОВНЫХ ПРОЦЕССАХ: ОБЗОР ИССЛЕДОВАНИЙ ПО ЦИФРОВОЙ КРИМИНАЛИСТИКЕ

DETECTING DIGITAL FOOTPRINTS IN VIRTUAL CRIMINAL PROCESSES: A REVIEW OF DIGITAL FORENSICS STUDIES

Таавалдыев Кылычбек
Таавалдыев Кылычбек
Taavaldyev Kylychbek

Кыргыз-Түрк Манас Университети
Кыргызско-Турецкий университет «Манас»
Kyrgyz-Turkish Manas University
2251y01001@manas.edu.kg

Исмаилова Рита
Исмаилова Рита
Ismailova Rita

Кыргыз-Түрк Манас Университети
Кыргызско-Турецкий университет «Манас»
Kyrgyz-Turkish Manas University
rita.ismailova@manas.edu.kg

ВИРТУАЛДЫК КЫЛМЫШ ПРОЦЕССТЕРИНДЕ САНАРИПТИК ИЗДЕРДИ АНЫКТОО: САНАРИПТИК КРИМИНАЛИСТИКАЛЫК ИЗИЛДӨӨЛӨРГӨ СЕРЕП САЛУУ

Аннотация

Технология өнүккөн сайын кылмыш дүйнөсү да өсүүдө. Виртуалдык дүйнө азыр кылмышкерлер жана укук коргоо органдары үчүн жаңы күрөш майданы болуп калды. Санариптик криминология - бул киберкылмыштуулукту жасоо учурунда пайда болгон санариптик издерди табууга жана анализдөөгө багытталган тез өсүп жаткан тармак катары белгилүү. Бул обзордук макалада санариптик криминологияда “виртуалдык” дүйнөдө кылмыш процесстери учурунда түзүлгөн санариптик издерди аныктоо, талдоо жана чечмелөө үчүн колдонулган негизги түшүнүктөр жана ыкмалар жөнүндө жалпы маалымат берилет.

Ачкыч сөздөр: санариптик криминалистика, киберкылмыштуулук, санариптик издер, маалыматтарды талдоо, куралдар жана техникалар.

ОБНАРУЖЕНИЕ ЦИФРОВЫХ СЛЕДОВ В ВИРТУАЛЬНЫХ УГОЛОВНЫХ ПРОЦЕССАХ: ОБЗОР ИССЛЕДОВАНИЙ ПО ЦИФРОВОЙ КРИМИНАЛИСТИКЕ

Аннотация

По мере развития технологий развивается и криминальный мир. Виртуальный мир теперь стал новым полем битвы для преступников и правоохранительных органов. Цифровая криминология — это быстро развивающаяся область, которая занимается поиском и анализом цифровых следов, созданных во время совершения киберпреступлений. В данной обзорной статье представлен обзор основных концепций и методов, используемых в цифровой криминалистике для выявления, анализа и интерпретации цифровых следов, созданных в ходе уголовного судопроизводства в «виртуальном» мире.

Ключевые слова: цифровая криминалистика, киберпреступность, цифровые следы, анализ данных, инструменты и методы.

DETECTING DIGITAL FOOTPRINTS IN VIRTUAL CRIMINAL PROCESSES: A REVIEW OF DIGITAL FORENSICS STUDIES

Abstract

As technology advances, so does the criminal world. The virtual world has now become a new battleground for criminals and law enforcement agencies. Digital forensics is a rapidly growing field that focuses on finding and analyzing digital traces created during the commission of cybercrime. This review article provides an overview of the basic concepts and methods used in digital forensics to identify, analyze, and interpret digital traces created during criminal proceedings in a "virtual" world.

Keywords: Digital Forensics, Cybercrime, Digital Traces, Data Analysis, Tools and Techniques.

Киришүү

Санариптик криминология - бул информатика, криминалистика, укук жана криминология сыяктуу ар кандай экспертиза чөйрөлөрүнө таянган мультидисциплинардык тармак (Holt et al., 2022). Санариптик дүйнө, киберкылмышкерлерди изин табуу үчүн чогултууга, талдоого жана далил катары колдонула турган көптөгөн маалыматтарды сунуштайт (Paul Joseph & Norman, 2020).

Учурда санариптештирүү күчөгөн сайын кылмыштуу аракеттер да виртуалдык дүйнөгө өтүп жатат. Купуялыкты камсыз кылган жана анонимдүүлүктү сактаган куралдар жана ыкмалар кылмышкерлердин санариптик чөйрөдө иштөөсүн бир топ эле жеңилдетти (Baykara et al., 2013). Бул өз кезегинде кибермейкиндиктеги кылмыштуу ишмердүүлүктүн санариптик изин табуу жана кылмышкерлерди жоопкерчиликке тартуу милдетин дагы да татаалдаштырат.

Жашыруун электрондук почта эсептеринен кол салуу (Ghafarian, 2020), банк эсептерине кибер чабуулдар (Mariani et al., 2023) жана ушул сыяктуу кылмыштуу аракеттер санариптик криминалисттердин эксперттери туш болгон негизги көйгөйлөрдүн бири. Мындай чабуулдарды жасоодо кылмышкерлер ар кандай ыкмаларды жана методдорду колдонуу менен санариптик издерди жашырууга же жок кылууга аракет кылышат. Бул жагдай окуяны жана санариптик далилдерди иликтөө процессин кыйындатат жана эксперттердин бул кылмыштарды иликтөө жана кылмышкерлерди аныктоо аракеттерине тоскоол болот.

Анткени, санариптик издерди чогултуу, талдоо жана чечмелөө көйгөйлөрү татаал болушу мүмкүн (Paul Joseph & Norman, 2020), өнүккөн куралдарды жана ыкмаларды талап кылат (S. Singh & Kumar, 2020). Бул серептөө, обзордук макаласында кылмыштын виртуалдык дүйнөсүндөгү санариптик издерди аныктоо жана талдоо үчүн санариптик криминологияда колдонулган түшүнүктөрдү, куралдар жана ыкмаларды изилдейт.

Андан сырткары, санариптик криминологиянын негизги түшүнүктөрүн жана ыкмаларын карап чыгуу менен "виртуалдык" дүйнөдө болуп жаткан кылмыш процесстеринин жүрүшүндө түзүлгөн санариптик издерди аныктоо жана талдоо үчүн колдонулган ыкмаларды киргизүүгө багытталган. Бул макалада санариптик криминологиянын маанилүүлүгү баса белгилөө менен, санариптик издердин маанилүүлүгү түшүндүрүлөт, колдонулган инструменттер жана ыкмалар жөнүндө маалымат берилип, санариптик криминологиянын этикалык жана укуктук аспектилери талкууланат. Бул обзордук макаланын жыйынтыгы, санариптик криминология тармагында иштеген изилдөөчүлөр, студенттер жана кызыкдар тараптар үчүн маалымдама булагы катары кызмат кылат.

Метод жана материалдар

Изилдөө суроолору

Бул макаланын максатына жетүү үчүн, башкача айтканда санариптик издерди аныктоо жана талдоо үчүн колдонулган ыкмаларды аныктоо максатында төмөнкү изилдөө суроолору коюлган.

1 изилдөө суроо - Санариптик издерди аныктоо үчүн кандай аспаптар жана ыкмалар колдонулат? Тактап айтканда,

- Санариптик издерди талдоо үчүн кандай маалыматтарды талдоо аспаптары жана ыкмалары колдонулат?
- Санариптик криминология изилдөөлөрүндө колдонулган маалыматтардын тактыгы жана ишенимдүүлүгү кантип камсыз кылынат?

2 изилдөө суроо - Дүйнөлүк тажрыйба боюнча кандай изилдөөлөр бар?

3 изилдөө суроо - Санариптик криминология жаатында учурда Кыргызстандагы абал кандай?

Процедуралар

Сереп салынган баардык булактар, макалалар Google Scholar издөө системасындан каралды, ал эми издөөнү женилдетүү жана маалыматка бат жетүү максатында Digital Criminology, Cybercrime жана Digital Traces ачкыч сөздөрү колдонулду. Google Scholar'та издөөнү так жана максаттуу кылуу үчүн платформа сунуш кылган бир нече стратегиялар жана функциялар колдонулган. Биз так дал келүүлөрдү издөө үчүн тырмакча (" ") сыяктуу өркүндөтүлгөн издөө операторлорун колдондук. Мисалы, "Digital Criminology" так ошол фразасы бар макалаларды гана чыгарат. Жалпысынан бул стретегия менен издөө жыйынтыктары бизге ар биз ачкыч сөз менен 649 макала (Digital Criminology ачкыч сөзү үчүн), 180 000 макала (Cybercrime) жана 19 700 макала (Digital Traces) чыгарылды.

Ошондуктан экинчи кадамда бул ачкыч сөздөрдү аналитикалык аспап тарабы үчүн Data Analysis, Tools and Techniques жана Legal and Ethical Considerations сөздөрү менен комбинациялыра каралды. Жыйнынтыкта чыккан макалалардын саны:

- "Digital Criminology", Data Analysis – 517 жыйынтык,
- "Digital Criminology", Tools and Techniques – 310 жыйынтык,
- "Digital Criminology", Legal and Ethical Considerations – 307 жыйынтык,
- "Cybercrime", Data Analysis – 69000 жыйынтык,
- "Cybercrime", Tools and Techniques – 45700 жыйынтык,
- "Cybercrime", Legal and Ethical Considerations – 19500 жыйынтык,
- "Digital Traces", Data Analysis – 17400 жыйынтык,
- "Digital Traces", Tools and Techniques – 10200 жыйынтык,
- "Digital Traces", Legal and Ethical Considerations – 7120 жыйынтык,

Экинчи кадамдын жыйынтыгы боюнча, үчүнчү кадамда үчтүк жана төртүк комбинациялар каралып, арасынан диссертация жана патенттер чыгарылды, жана жыйынтыктар саны 150 макалага төмөндөдү.

Төртүнчү кадамда макалалар контент анализине алынып, натыйжада 55 макала тандалды.

Материалдар

Жогоруда айтылгандай, изилдөө үчүн 55 макала колдонулуп жалпысынан 119 автордон, 2013-2024-жж аралыгын камтыйт. Сереп салынган баардык булактар, макалалар Google Scholar издөө системасындан каралды.

Бул макалалар киберкоопсуздук чөйрөсүндөгү маалыматтын кеңири спектрин камсыз кылат, кибер чабуулдардын ар кандай аспектилерин жана аларга каршы чечимдерди камтыйт. Алардын ар бири темага ар башка көз караш менен кайрылып, санариптик дүйнөнүн татаалдыгын жана коопсуздуктун алсыздыгынын олуттуулугун баса белгилешет. Ага кошумча санариптик кылмыштуулуктун этикалык маселелерине да токтолуп өтөт. Бул макалалар санариптик чөйрөдө коопсуздукту камсыз кылуу үчүн иштелип чыккан техникалардын жана стратегиялардын маанилүүлүгүн баса белгилеп, кибер коопсуздук жаатындагы изилдөөлөргө жана тажрыйбаларга шилтеме берет.

Бул ресурстар киберчабуулдар жана санариптик криминология боюнча кеңири маалыматты берет. Макалалардын айрымдары киберкоопсуздукка багытталган, ал эми башкалары санариптик криминалистикага жана санариптик издерди аныктоо ыкмаларына багытталган.

Жыйынтыктар

Санариптик криминологиянын негизги түшүнүктөрү

Жалпы терминдер

Санариптик криминология – бул “виртуалдык” дүйнөдө кылмыш процесстери жүрүп жаткан санариптик чөйрөлөрдө болгон кылмыштарды текшерүү жана бул кылмыштардын санариптик изин аныктоо менен алектенген дисциплина (Arakerimath & Gupta, 2015). Санариптик криминология, санариптик чөйрөлөргө салттуу криминология принциптерин колдонуу менен кылмыштардын алдын алууга, кылмышкерлерди табууга жана соттоого салым кошот. Бул дисциплина санариптик технологиялардын тез өнүгүшү менен барган сайын көбүрөөк мааниге ээ болууда. Бүгүнкү санариптик доордо уюшкан кылмыштуу топтор технологиялык жетишкендиктерди пайдаланууга ыңгайлаштырууда. Бул топтор салттуу кылмыштуу уюмдардан кибер кылмыштуу тармактарга чейин жана азыр адамдар менен машиналар тыгыз иштешкен санариптик чөйрөдө иштешет (Di Nicola, 2022).

Санариптик криминологиянын негизги түшүнүктөрү бул тармакта иштегендер үчүн маанилүү көрсөтмөлөрдү берет жана санариптик кылмыштарды түшүнүүгө өбөлгө түзүп берет. Алгач, санариптик кылмыш терминин карай турган болсок, бул термин санариптик криминологиянын маанилүү чөйрөсү жана компьютерлерди, интернетти жана башка санарип технологияларды колдонуу менен жасалган ар кандай кылмышы түшүндүрөт (Holt et al., 2022). Мындай кылмыштар хакерлик (Buchanan, 2020), фишинг (Aslam & Nassif, 2023), онлайн куугунтук, маалыматтардын сыртка чыгышы (van der Kleij et al., 2020) жана онлайн алдамчылык сыяктуу ар кандай аракеттерди камтышы мүмкүн. Ал эми компьютердик системаларга уруксатсыз кирүү жана манипуляциялоо актысы болгон хакердик санариптик криминологиянын кызыгуу чөйрөсү болуп саналат жана бул тармакта адистешүү маанилүү

(Marin et al., 2021). Хакердик кылмыштарды иликтөө жана алдын алуу үчүн түрдүү ыкмалар иштелип чыгууда. Мындан тышкары, санариптик кылмыштарды комплекстүү чечүү үчүн структураланган санариптик криминалистикалык ыкмаларга багытталган жаңы киберкылмыштарды иликтөө модели киргизилген (Ivanova & Stefanov, 2023; Sangwan, 2022). Бирок, хакердик менен күрөшүү бул санариптик кылмышты иликтөөнүн бир гана бөлүгү.

Бул түр кылмыштардан кордоо тарабын карай турган болсок, санариптик мониторинг жана байкоо жүргүзүү ыкмалары бул кылмыштарды иликтөөдө жана алдын алууда маанилүү роль ойнойт (Kotari & Chiplunkar, 2020). Бул ыкмалар кылмыштарды жана кылмышкерлерди аныктоо жана далилдерди чогултуу (Milenkovic, 2023) үчүн колдонулат. Кылмыштын бетин ачуу жана кылмышкерлерди жоопкерчиликке тартуу үчүн техникалык билимдин өзү эле жетишсиз болушу мүмкүн, анткени бул процесстер көбүнчө көп катмарлуу жана бир нече дисциплиналарды камтыйт (Jacob et al., 2020).

Санариптик далилдер кылмыштарды ачуу жана кылмышкерлерди куугунтуктоо үчүн абдан маанилүү. Бул далил компьютер файлдарын, электрондук почталарды, текст кабарларды, интернет тарыхын жана башка санарип жазууларды камтышы мүмкүн (Semko & Krakhmalyov, 2023). Бирок, бул далилдерди чогултуу, талдоо жана көрсөтүү татаал процесс (Paul Joseph & Norman, 2020) жана аны туура иштетүү керек.

Андан сырткары, санариптик криминология изилдөөлөрүндө санариптик купуялуулук жана этикалык маселелер да маанилүү ролду ойнойт (Winter & Gundur, 2024). Кылмыштуулук менен күрөшүүдө адамдардын жеке жашоосун коргоо жана этикалык нормаларды сактоо маанилүү. Бирок, бул маселелерди чечүүдө этият болушу керек жана адилеттүүлүктү сактоо менен тең салмактуу болушу керек.

Санариптик криминология технологиянын тез өзгөрүп турган табиятынан улам тынымсыз өнүгүп келе жаткан тармак. Ошондуктан, бул негизги түшүнүктөр тынымсыз кайра каралып, жаңыланып турат. Бирок, бул түшүнүктөр санариптик кылмыштар менен күрөшүүдө натыйжалуу иш-аракет үчүн негизги негиз болуп саналат.

Санариптик издердин маанилүүлүгү жана аныктоо үчүн колдонулган куралдар

Санариптик издер бул кылмыш процесстери учурунда санариптик маалымат каражаттарында калтырылган электрондук далилдер (Baykara et al., 2013). Бул издер кылмышкерлерди аныктоодо, кылмыштарды далилдөөдө жана сот процессинде колдонулат. Санариптик криминологияда колдонулган инструменттер санариптик издерди аныктоо жана талдоо үчүн маанилүү ролду ойнойт. Аларга санарип далилдерди чогултуу программасы (C. Singh et al., 2022), маалыматтарды калыбына келтирүү куралдары (Tomer et al., 2017), маалыматтарды талдоочу программалык камсыздоо жана санариптик коопсуздук куралдары кирет.

Кибер коопсуздук чөйрөсү учурда барган сайын маанилүү болуп баратат. Тез өнүгүп жаткан технология менен санариптик дүйнөдө коркунучтар да көбөйүүдө. Бул кооптонуулар менен күрөшүү жана маалыматтык коопсуздукту камсыз кылуу үчүн ар кандай инструменттер жана ыкмалар колдонулат. Киберкоопсуздук куралдары - бул тармактарды, системаларды

жана маалыматтарды коргоо жана коркунучтарды, кылмышкерлердин изин аныктоо жана аларга жооп берүү үчүн колдонулган программалык камсыздоо.

Буга байланыштуу киберкоопсуздук боюнча эксперттер жана адистер тарабынан куралдардын кеңири спектри колдонулат. Бул инструменттер тармакты сканерлөө жана чалгындоодон аялуу жерлерди аныктоого, зыяндуу программаларды жок кылууга жана санариптик далилдерди изилдөөгө чейин ар кандай максаттар үчүн иштелип чыккан.

Төмөндө, киберкоопсуздук жана электрондук криминалистика тармагында кеңири колдонулган куралдардын талдоосу төмөндө келтирилди.

Жадыбал 1. Адабият талдоо жыйынтыктары

Куралдар	**Колдонуу чөйрөсү**	**Акысы**	**Артыкчылыгы**	**Кемчилиги**
1. Wireshark (Iqbal & Naaz, 2019)	Тармак анализи	Акысыз	Кеңири протоколдук колдоо, колдонууга оңой	Жогорку трафикте начар көрсөткүч
2. Metasploit (Balajinarayan, 2019)	Penetrasion тест	Акылуу	күчтүү эксплойт жана чабуул сценарийлери	Акы төлөнүүчү версия көбүрөөк функционалдуу
3. Nmap (Mohammed et al., 2022)	Тармакты табуу жана сканерлөө	Акысыз	Тез жана натыйжалуу тармак сканерлөө	Кээ бир Firewall дор аркылуу аныктоого болот
4. Burp Suite (Kore et al., 2022)	Веб тиркеме тести	Акылуу	Комплекстүү веб-тиркеме тестирлөө куралдары	Жогорку баа
5. Snort (Tudosi et al., 2022)	Тармактык мониторинг жана кол тамга тести	Акылуу	Кол тамгага негизделген чабуулду бат аныктоо	Жогорку денгээлдеги туура эмес позитивдүү ката өлчөмү
6. John the Ripper (Marchetti & Bodily, 2022)	Сырсөз бузуу	Акылуу	Бир нече сырсөздү бузуу мүмкүнчүлүктөрү	Кээ бир татаал сырсөздөрдү бузуудагы кыйынчылык
7. Maltego (Schwarz & Creutzburg, 2021)	Маалымат чогултуу жана талдоо	Акылуу	Графиктердин негизинде маалыматтарды чогултуу жана талдоо	Колдонуучуга ыңгайлуу эмес
8. Aircrack-ng (John et al., n.d.)	Зымсыз тармак коопсуздугу	Акылуу	Зымсыз тармактарда аялууларды аныктоо жана кол салуу	Орнотуу жана колдонуу татаал
9. MailXaminer (Ghafarian, 2020)	электрондук почта анализи	Акылуу	Комплекстүү электрондук почта анализи мүмкүнчүлүктөрү	Колдонуучу интерфейси бир аз татаал

10. Forensic Toolkit (FTK) (Altulaihan et al., 2023)	Санариптик изилдөө	Акылуу	файл форматын колдоо	Жогорку система талаптары

Бул куралдар киберкоопсуздук боюнча эксперттерге ар кандай коркунучтар менен күрөшүүгө жана алардын тармактарын коопсуз сактоого жардам берсе, электрондук почтанын криминалистикасынын куралдары электрондук почта трафигин текшерүү, контент анализи, email header анализи менен кылмыштарды аныктоого жана санариптик далилдерди чогултууга жардам берет. Бирок, ар бир курал артыкчылыктары жана кемчиликтери бар. Кээ бирлери колдонуучуга ыңгайлуу интерфейстер менен келет, ал эми башкалары татаал конфигурацияга же кымбатка турат (Жадыбал 1.).

Натыйжада, киберкоопсуздук жана электрондук криминалистика тармагында колдонулган инструменттер санариптик дүйнөдөгү коопсуздук көйгөйлөрү менен күрөшүүдө маанилүү ролду ойнойт. Бирок, бул куралдар этикалык жана укуктук стандарттарга ылайык колдонулушу маанилүү жана колдонуучулар бул куралдарды колдонууда этият болушу керек(Winter & Gundur, 2024).

Мындан тышкары, санарип криминология изилдөөлөр этикалык жана укуктук аспектилери каралышы керек болгон аймак болуп саналат. Маалыматтын купуялыгы, маалыматтардын коопсуздугу, маалымат алмашуу жана юридикалык процесстер сыяктуу маселелер санариптик криминологияны изилдөөдө каралышы керек болгон этикалык жана укуктук аспектилер болуп саналат (Winter & Gundur, 2024). Изилдөөчүлөр бул маселелер боюнча этикалык эрежелерди жана укуктук ченемдерди сактоого тийиш.

Санариптик криминологиянын изилдөөлөрүнүн көйгөйлөрү жана келечеги

Санариптик криминологияны изилдөөнүн алдында турган кыйынчылыктар жана мүмкүнчүлүктөр ар түрдүү. Тез өнүгүп жаткан социалдык чындык (social reality) реалдуу убакыт режиминде кылмыштуу көрүнүштөрдү көзөмөлдөө үчүн «сандык криминология парадигмасына» жана «эсептөөчү криминологияга» өтүүнү талап кылат (Приколотина, 2022)

Санариптик кылмыштардын өсүп келе жаткан татаалдыгы, учурдагы криминологиялык ыкмаларга критикалык баа берүүнү жана санариптик кылмыштарга каршы күрөшүүнүн теориялык негизин иштеп чыгууну талап кылат (Serebrennikova & Serebrennikova, 2021; Серебренникова, 2020). Санариптик криминалистика санариптик кылмыш иш-аракеттерин жана киберчабуулдарды иликтөөдө маанилүү ролду ойнойт жана санариптик иликтөөдө эффективдүү методдор менен куралдардын зарылдыгын баса белгилейт (Khan et al., 2022). Кошумчалай кетсек, санариптик байланыштын теңтуштардын таасирине (Peer influence) жана кылмыштуулукка тийгизген таасири оффлайн механизмдердин кибермейкиндикке кеңейүүсүн баса белгилейт жана кылмыштуу жүрүм-турумду түшүнүү үчүн жаңы чакырыктарды жана мүмкүнчүлүктөрдү берет (McCuddy, 2022). Санариптик криминология боюнча изилдөөлөрдүн келечеги бул көйгөйлөрдү инновациялык методологиялар жана теориялык негиздер аркылуу чечүүдө турат. Буга байланыштуу

изилдөөлөр жаңы ыкмаларды иштеп чыгууга, биргелешкен тармактарды түзүүгө жана этикалык стандарттарды бекемдөөгө басым жасашы керек.

Андан сырткары, санариптик криминологияны изилдөөдө кээ бир кыйынчылыктарга туш болушу мүмкүн. Буларга техникалык татаалдык, тез өзгөрүүчү технологиялар, маалыматтардын көптүгү, маалыматтардын тактыгы жана кызматташуунун жоктугу сыяктуу факторлор кирет. Келечекте санариптик криминология чөйрөсү дагы көбүрөөк мааниге ээ болот деп күтүлүүдө. Бул чөйрөдөгү изилдөөлөр жаңы техникаларды иштеп чыгууга, кызматташуу тармактарын түзүүгө жана этикалык стандарттарды бекемдөөгө багытталышы керек.

Колдонуу аймактары жана мисалдар

Санариптик криминологияны изилдөөнүн колдонуу чөйрөлөрү абдан кеңири. Бул аймактарда кибер кылмыштуулук, санариптик алдамчылык, балдарга карата зордук-зомбулук, маалыматтарды бузуу жана хакерлик сыяктуу маселелер кирет.

Киберкылмыш ар кандай ыкмалар, анын ичинде фишинг, бөлүштүрүлгөн кызматтан баш тартуу (DDoS), кесепеттүү программаларды жайылтуу жана башкалар аркылуу ишке ашырыла турган чабуул ыкмаларын камтыйт. Киберкылмыштарды иликтөө көбүнчө тармактык трафикти талдоо, санариптик мониторинг, маалыматтарды көзөмөлдөө жана киберкоопсуздук куралдарын колдонууну камтыйт. Кошумчалай кетсек, кибер кылмыштуулуктун алдын алуу үчүн кирүү тесттери жана аялуу жерлерди сканерлөө сыяктуу активдүү чаралар көрүлүшү мүмкүн. Мисалы, 2014-жылы Yahoo системаларына жасалган чабуулдун жыйынтыгында хакерлер 500 миллион колдонуучунун маалыматтарын уурдап кетишкен (Daswani & Elbayadi, 2021). Фишингдик чабуулдар адамдардын жеке маалыматтарын зыяндуу максаттарда колдонууга багытталган киберкылмыштуулуктун кеңири таралган түрү катары белгиленет (Aslam & Nassif, 2023; Bhavsar et al., 2018).

Бул кылмыштардын алдын алуу жана кылмышкерлерди жоопко тартуу боюнча натыйжалуу стратегияларды иштеп чыгуу санариптик криминология тармагынын орчундуу максаты болуп саналат. Бул жагынан алганда, тиешелүү колдонуу ыкмаларын колдонуу жана тынымсыз жаңыланып жаткан технологиялык куралдар менен колдоого алынган изилдөөлөрдү жүргүзүү санариптик криминологияны өнүктүрүүгө жана анын кылмыштуулукка каршы күрөшүүдөгү натыйжалуулугуна өбөлгө түзөт. Тергөөчүлөр киберкылмыштарды алдын алуу жана чабуул жасагандарды аныктоо үчүн маалыматтарды талдоо, санариптик мониторинг, кибер коркунучтарды чалгындоо жана санариптик криминалистика ыкмалары сыяктуу түрдүү куралдарды колдонушат.

Дүйнөлүк тажрыйба

Киберкоопсуздук кылмыштары боюнча глобалдык изилдөөлөр улуттук жана эл аралык деңгээлдеги көйгөйлөрдүн көбөйүп жатканын көрсөтүп турат. Бул жаттагы адабияттар киберкылмыштуулук менен натыйжалуу күрөшүү үчүн эл аралык кызматташтыктын жана күчтүү укук коргоо органдарынын маанилүүлүгүн баса белгилейт (Sumadinata, 2023). Изилдөөлөр эл аралык, улуттук, институционалдык жана жеке деңгээлдеги ар кандай көз

караштарды карап чыгуу менен киберкоопсуздуктун глобалдык тенденцияларын жана өнүгүүлөрүн талдоого багытталган (Dhawan et al., 2021)

Бирок, изилдөөлөр киберкылмыштуулуктун татаалдыгына басым жасап, бул жаатта түшүнүктөрдү жана тажрыйбаларды бөлүшүүнүн маанилүүлүгүн баса белгилөө менен, андан аркы изилдөөлөрдү колдоду (Moneva et al., 2023). Киберчабуулдардын жайылышы, өзгөчө COVID-19 пандемиясынан улам санариптик трансформациянын ылдамдашы менен системалуу изилдөөлөрдү жана эксперттик корутундуларды эске алуу менен кол салуу ыкмаларын аныктоого жана коргоо фреймворторун иштеп чыгууга алып келди (Verma & Shri, 2022). Кошумчалай кетсек, ар кайсы өлкөлөрдө киберкоопсуздукту кабылдоо жана тенденциялары боюнча изилдөөлөр веб-майнинг жана машина үйрөнүү ыкмаларын колдонуу менен жүргүзүлгөн (Quisumbing, 2017).

Киберкылмыштуулук боюнча аткарылган изилдөөлөрдү карап чыга турган болсок, киберкылмыш ииздерин социалдык тармактарда (Scanlon, Breitinger, et al., 2023), IoT - нерселердин интернетинде (Alazab et al., 2023), метаверс (Metaverse) планформаларында (Seo et al., 2023), блокчейн технологияларды колдонуу менен иштелип чыккан системаларда (Ramazhamba & Venter, 2023) ж.б.у.с. технологияларды издөө боюнча көптөгөн изилдөөлөр аткарылганын көрө алабыз. Мисалы, Chrome веб-браузеринде Discord деп аталган социалдык медиа тиркемесинин калдыктарын карап чыккан изилдөөдө, жөнөкөй тексттеги артефакттар Google Chrome сактагыч жерлеринен, кэш жана башка көптөгөн жерлерден алынаарын аныктаган (Gupta et al., 2023). Авторлор бул ыкма менен төлөм маалыматы, жөнөтүлгөн билдирүүлөр, эсеп жөндөөлөрү, сүйлөшүүлөр, жүктөлгөн тиркемелер жана башка көптөгөн артефакттарды калыбына келтиргенин жана бул топтолгон маалыматтын бардыгын соттук иликтөөдө колдонууга болоорун айтууда.

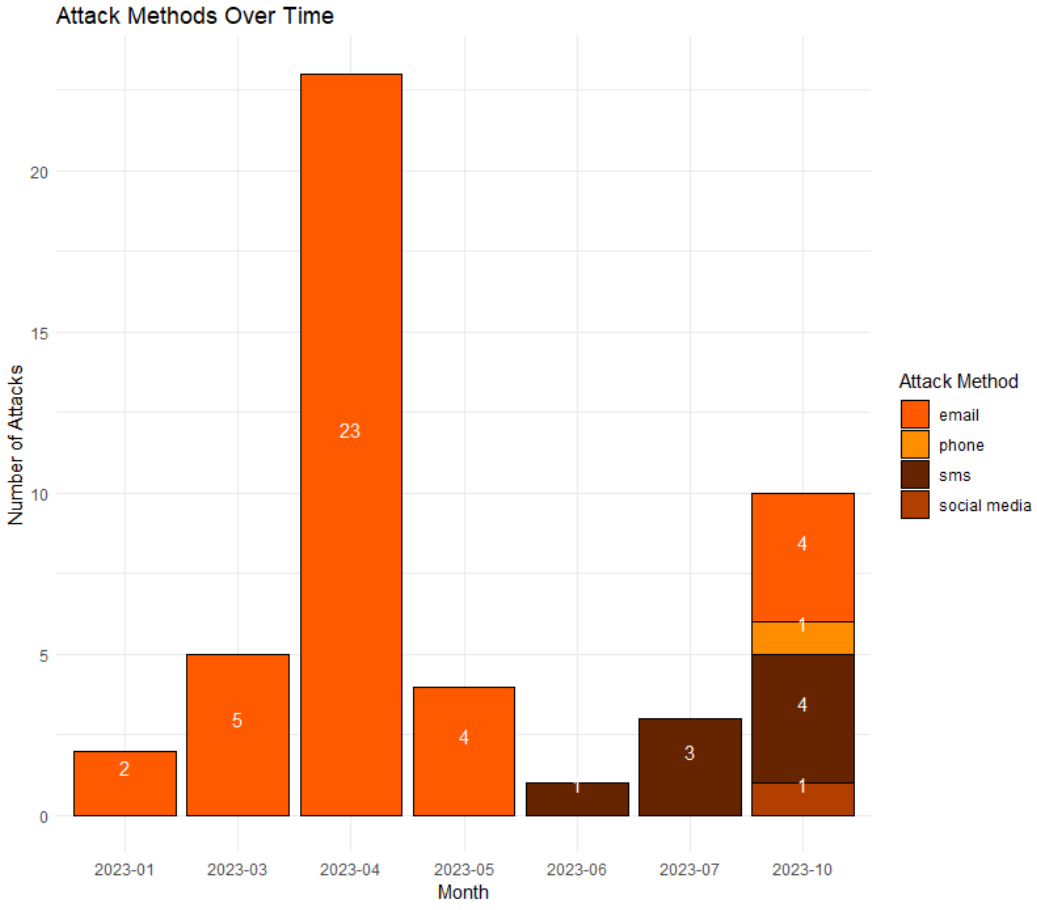
Ал эми кылмыш издерин топтоо ыкмалары жана аспаптарга өтө турган болсок, ыкмалар көбүнчө физикалык жана санариптик далилдерди аныктоону, сактоону жана талдоону камтыганы айтылат (Alazab et al., 2023).

Санарип криминалистикасында бир нече кыйынчылыктар бар экенин дагы көптөгөн изилдөөчүлөр баса белгилөөдө. Көбүнчө кыйынчылыктар, азыркы технологиялар татаал жана өнүгүп жаткан тармакка айланганынан чыгып келгенин айтууда (Alazab et al., 2023). Мисалы, нерселердин интернетиндеги негизги көйгөйлөрдүн бири - нерселер түзмөктөрүнүн жана алардын ар кандай операциялык системаларынын, аппараттык конфигурацияларынын жана байланыш протоколдорунун көп түрдүүлүгү. Мунун тышында, акыркы учурда жасалма интеллекттин өнүгүшү дагы киберкылмыштуулук аренасын өтө кескин түрдө алмаштыруусу дагы көптөгөн изилдөөчүлөрдүн көңүлүн бурууда (Scanlon, Breitinger, et al., 2023; Scanlon, Nikkel, et al., 2023). Кошумчалай кетсек, маалымат технологиялар тармагында стандартташтыруунун жана жөнгө салуунун жоктугу бул түзмөктөрдөн алынган соттук далилдердин аныктыгын жана ишенимдүүлүгүн аныктоону кыйындатканын изилдөөчүлөр баса белгилөөдө.

Кыргызстандагы учурдагы абал

Өлкөлөрдүн киберкоопсуздук абалы алардын өнүгүү деңгээлине жана ресурстарына жараша ар кандай болушу мүмкүн. Өнүккөн өлкөлөр жалпысынан киберкоопсуздуктун күчтүү инфраструктураларына, жогорку технологиялык компетенцияларга жана киберкоопсуздук боюнча маалымдуулукка жетилген мамилеге ээ болсо да, өнүгүп келе жаткан өлкөлөр же айрым географиялык аймактардагы өлкөлөр чектелген ресурстарга жана инфраструктуралык кемчиликтерге туш болушу мүмкүн.

Айрыкча, Кыргызстан сыяктуу өлкөлөр электрондук почта чабуулдарына дуушар болушу мүмкүн. Кыргызстанда электрондук почта аркылуу жөнөтүлгөн коркутуп-үркүтүүчү билдирүүлөрдүн көрсөткүчү 79,2%ды түзгөнү аныкталган (Kaktus.Kg, 2023). Бул өлкөнүн киберкоопсуздук инфраструктурасынын чектелгендигинен же киберкоопсуздук боюнча жетишсиз маалымдуулугунан улам, электрондук почта чабуулдарына көбүрөөк алсыз болуп калганын көрсөтүп турат.



Сүрөт 1. Кактус Медиа тарабынан 2023-жылы Бомба кабары тууралуу Кыргызстанда жарыяланган маалыматтарга негизделген чачыранды диаграмма.

Электрондук почта, социалдык медиа жана байланыш тиркемелери сыяктуу ар кандай байланыш каналдары аркылуу коркунучтарды талдоо кибер коопсуздук саясатын иштеп чыгууда жана коргонуу стратегияларын түзүүдө абдан маанилүү. Кыргызстанда жүргүзүлгөн изилдөөлөр көрсөткөндө (Сурөт 1), электрондук криминалистика санариптик криминалистика

тармагында маанилүү роль ойнойт. Изилдөөнүн бул түрү киберкылмыштуулук жана коркунучтар байланыш каналдарына жараша кандайча өзгөрүп жана айырмаланарын түшүнүү үчүн маанилүү. Бул өз кезегинде Кыргызстан сыяктуу өлкөлөрдө электрондук почтанын криминалистикасына көңүл буруу кибер кылмыштуулукка каршы күрөшүүдө эффективдүү стратегияларды аныктоого салым кошо алат.

Айрыкча, мындай байланыш каналдарын туура эмес колдонууга байланыштуу фишинг сыяктуу киберчабуул ыкмаларын да баса белгилеп кетүү зарыл. Фишинг – бул колдонуучулардын жеке маалыматын алуу үчүн адаштырууга багытталган социалдык инженердик чабуулдун бир түрү (Qabajeh et al., 2018). Мындай чабуулдар жасалма веб-сайттар же жасалма электрондук почта даректери аркылуу ишке ашырылып, колдонуучуларды хакерлер тарабынан көзөмөлдөнгөн зыяндуу мазмунга дуушар кылышы мүмкүн. Андыктан киберкылмыштуулук менен күрөшүүдө колдонуучулардын маалымдуулугун жогорулатуу жана түшүндүрүү иштери да маанилүү.

Фишинг сыяктуу ыкмалар олуттуу коркунуч туудураарын эске алып, каржы мекемелери менен колдонуучулардын ортосундагы ишенимди камсыз кылуу үчүн чаралар көрүлүгө тийиш. Мисалы, DemirBank сыяктуу мекемелер өз кардарларын мындай алдамчылык аракеттерине каршы маалымдайт (Demirbank.Kg, 2024). Банк колдонуучуларга DemirBanktын жасалма эсептери жана алдамчылык аракеттери тууралуу эскертүү менен кардарларга өздөрүнүн жеке маалыматтарын коргоого жардам берет. Мындай эскертүүлөр кардарларды кабардар кылып, алардын киберкылмышкерлердин алдамчылык аракеттерин таанууга жана сактык чараларын көрүүгө өбөлгө түзөт.

Акыркы учурда көбөйгөн фишинг чабуул аракеттеринен улам, Кыргыз Республикасынын Жеке маалыматтарды коргоо боюнча мамлекеттик агенттик маалым кат чыгарган (Economist.kg, 2024). Андан сырткары Оптима Банк кардарларына жасалма веб-сайттар жана алдамчылык издөө менен көбөйүп кеткен алдамчылык фактыларынан этият болууга кеңеш берет жана кардарлардын жеке маалыматтары менен бөлүшпөөгө, шектүү шилтемелерге чыкпоого жана шектүү издөөлөрдөн этият болууга чакырат (OptimaBank, 2024). Ага кошумча учурда киберчабуул жасоого аракет жасагандардын күн санап өнүгүп жаткандыгына байланыштуу банк кызматкерлери дайыма маалыматтык иш-чараларды өткөрүү менен бул маселе боюнча түшүндүрүү иштерин жүргүзүүдө. Алар жасалма сайттар аркылуу колдонуучуларды алдоо жолу менен колдонуучу маалыматын уурдоого аракет кылып жатышат деп билдирет. Ошондуктан, колдонуучулар банк тарабынан жөнөтүлгөн маалыматты бөлүшпөшү керек жана банктын расмий сайтын же мобилдик тиркемесин гана колдонуп, шектүү иш-аракеттер банкка дароо билдирилиши керектиги айтылат (Mbank, 2024).

Корутунду жана сунуштар

Санарип криминологиясы "виртуалдык" дүйнөдө болуп жаткан кылмыш процесстеринин жүрүшүндө түзүлгөн санариптик издерди аныктоо жана талдоо үчүн маанилүү дисциплина болуп саналат. Бул обзордук макалада санариптик криминологиянын негизги түшүнүктөрүн түшүндүрүү, колдонулган инструменттер жана ыкмалар, ошондой эле этикалык жана укуктук аспектилери жөнүндө маалымат берилди. Мындан тышкары, колдонуу аймактары жана кейс изилдөөлөр баса белгиленди. Санариптик криминология тармагында

иштеген изилдөөчүлөр, студенттер жана кызыкдар тараптар үчүн бул макала маалымдама булагы болуп калат.

Адабият

1. Alazab, A., Khraisat, A., Singh, S., Alazab, A., Khraisat, A., & Singh, S. (2023). *A Review on the Internet of Things (IoT) Forensics: Challenges, Techniques, and Evaluation of Digital Forensic Tools*. IntechOpen. https://doi.org/10.5772/intechopen.109840
2. Altulaihan, E., Alismail, A., Hafizur Rahman, M. M., & Ibrahim, A. A. (2023). Email Security Issues, Tools, and Techniques Used in Investigation. *Sustainability*, *15*(13), 10612.
3. Arakerimath, A., & Gupta, P. K. (2015). Digital footprint: Pros, cons, and future. *International Journal of Latest Technology in Engineering*, *4*(10), 52–56.
4. Aslam, S., & Nassif, A. B. (2023). Phish-identifier: Machine Learning based classification of Phishing attacks. *2023 Advances in Science and Engineering Technology International Conferences (ASET)*, 1–6. https://ieeexplore.ieee.org/abstract/document/10180869/
5. Balajinarayan, B. (2019). A Study on Metasploit Payloads. *International Journal of Cyber-Security and Digital Forensics*, *8*(4), 298–308.
6. Baykara, M., Daş, R., & Karadoğan, İ. (2013). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. *1st International Symposium on Digital Forensics and Security (ISDFS'13)*, *20*, 21. https://bgys.iku.edu.tr/sites/bgys/files/inline-files/Bilgi%20G%C3%BCvenli%C4%9Fi%20Sistemlerinde%20Kullan%C4%B1lan%20Ara%C3%A7lar%C4%B1n%20%C4%B0ncelenmesi_0.pdf
7. Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. *International Journal of Computer Applications*, *182*(33), 27–29.
8. Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press. https://books.google.com/books?hl=en&lr=&id=NE3SDwAAQBAJ&oi=fnd&pg=PP1&dq=hacker+attacks+network+security&ots=MEiekiV82y&sig=WyMvFub_j-G9AoR2gLOCKjO69Nw
9. Daswani, N., & Elbayadi, M. (2021). The Yahoo Breaches of 2013 and 2014. In N. Daswani & M. Elbayadi, *Big Breaches* (pp. 155–169). Apress. https://doi.org/10.1007/978-1-4842-6655-7_7
10. *Demirbank.kg*. (2024). Demirbank.Kg. https://demirbank.kg/ru/about/news/news-detail?slug=demirbank-33
11. Dhawan, S. M., Gupta, B. M., & Elango, B. (2021). Global Cyber Security Research Output (1998–2019): A Scientometric Analysis. *Science & Technology Libraries*, *40*(2), 172–189. https://doi.org/10.1080/0194262X.2020.1840487
12. Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y
13. Economist.kg. (2024, March 12). *Фишинг, социальная инженерия, кража данных. Как обезопасить себя от телефонных мошенников?* Economist.kg. https://economist.kg/pravo-znat/2024/03/12/fishingh-sotsialnaia-inzhienieriia-krazha-dannykh-kak-raspoznat-tieliefonnykh-moshiennikov/
14. Ghafarian, A. (2020). An empirical analysis of email forensics tools. *Available at SSRN 3624617*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3624617
15. Gupta, K., Varol, C., & Zhou, B. (2023). Digital forensic analysis of discord on google chrome. *Forensic Science International: Digital Investigation*, *44*, 301479. https://doi.org/10.1016/j.fsidi.2022.301479
16. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and digital*

forensics: An introduction. Routledge. https://www.taylorfrancis.com/books/mono/10.4324/9780429343223/cybercrime-digital-forensics-thomas-holt-adam-bossler-kathryn-seigfried-spellar
17. Iqbal, H., & Naaz, S. (2019). Wireshark as a tool for detection of various LAN attacks. *Int. J. Comput. Sci. Eng*, *7*(5), 833–837.
18. Ivanova, M., & Stefanov, S. (2023). Digital Forensics Investigation Models: Current State and Analysis. *2023 8th International Conference on Smart and Sustainable Technologies (SpliTech)*, 1–4. https://ieeexplore.ieee.org/abstract/document/10193176/
19. Jacob, J., Peters, M., & Yang, T. A. (2020). Interdisciplinary Cybersecurity: Rethinking the Approach and the Process. In K.-K. R. Choo, T. H. Morris, & G. L. Peterson (Eds.), *National Cyber Summit (NCS) Research Track* (Vol. 1055, pp. 61–74). Springer International Publishing. https://doi.org/10.1007/978-3-030-31239-8_6
20. John, E., Kalu, C., & Asuquo, P. (n.d.). *Comparative Performance Analysis Of Cybersecurity Tools On A Wireless Network With WPA2 Encryption*. Retrieved April 22, 2024, from http://www.jmest.org/wp-content/uploads/JMESTN42354196.pdf
21. *Kaktus.kg*. (2023). Kaktus.Kg. https://kaktus.kg/doc/11835_bishkektegi_mektepterge_yniversitetterge_kayradan_bomba_tyralyy_bildiryy_tyshty.html
22. Khan, A. A., Shaikh, A. A., Laghari, A. A., Dootio, M. A., Rind, M. M., & Awan, S. A. (2022). Digital forensics and cyber forensics investigation: Security challenges, limitations, open issues, and future direction. *International Journal of Electronic Security and Digital Forensics*, *14*(2), 124. https://doi.org/10.1504/IJESDF.2022.121174
23. Kore, A., Hinduja, T., Sawant, A., Indorkar, S., Wagh, S., & Rankhambe, S. (2022). Burp Suite Extension for Script based Attacks for Web Applications. *2022 6th International Conference on Electronics, Communication and Aerospace Technology*, 651–657. https://ieeexplore.ieee.org/abstract/document/10009116/
24. Kotari, M., & Chiplunkar, N. N. (2020). A Survey on Detection and Analysis of Cyber Security Threats Through Monitoring Tools. In *Handbook of Research on Intrusion Detection Systems* (pp. 77–104). IGI Global. https://www.igi-global.com/chapter/a-survey-on-detection-and-analysis-of-cyber-security-threats-through-monitoring-tools/251798
25. Marchetti, K., & Bodily, P. (2022). John the Ripper: An Examination and Analysis of the Popular Hash Cracking Algorithm. *2022 Intermountain Engineering, Technology and Computing (IETC)*, 1–6. https://ieeexplore.ieee.org/abstract/document/9796671/
26. Mariani, L. A., Ornelas, J. R. H., & Ricca, B. (2023). *Banks' Physical Footprint and Financial Technology Adoption*. Inter-American Development Bank, Department of Research and Chief Economist. https://www.aeaweb.org/conference/2024/program/paper/hBszrffn
27. Marin, E., Almukaynizi, M., Sarkar, S., Nunes, E., Shakarian, J., & Shakarian, P. (2021). *Exploring Malicious Hacker Communities: Toward Proactive Cyber-Defense*. Cambridge University Press. https://books.google.com/books?hl=en&lr=&id=BzMiEAAAQBAJ&oi=fnd&pg=PR9&dq=Ericsson,+Marin.,+Mohammed,+Almukaynizi.,+Soumajyoti,+Sarkar.,+Eric,+Nunes.,+Jana,+Shakarian.,+Paulo,+Shakarian.,+Edward,+G.,+Amoroso.+(2021).+Exploring+Malicious+Hacker+Communities:+Toward+Proactive+Cyber-Defense.+++&ots=DiRawunCjo&sig=0S92fW_I3Cl0WQQZz_YhicCFYa8
28. *Mbank*. (2024). https://www.cbk.kg/ru/news/1499
29. McCuddy, T. (2022). Digital Disclosure of Delinquency: Online Peers and the Sharing of Offline Crime. *Crime & Delinquency*, *68*(13–14), 2554–2580. https://doi.org/10.1177/00111287211067179
30. Milenkovic, D. (2023). CYBER SECURITY AND DATA COLLECTION. *Security Science Journal*, *4*(1), 102–118.
31. Mohammed, F., Rahman, N. A. A., Yusof, Y., & Juremi, J. (2022). Automated nmap toolkit.

2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), 1–7. https://ieeexplore.ieee.org/abstract/document/10088375/

32. Moneva, A., Leukfeldt, E. R., & Romagna, M. (2023). Fieldwork Experiences Researching Cybercriminals. In A. M. Díaz-Fernández, C. Del-Real, & L. Molnar (Eds.), *Fieldwork Experiences in Criminology and Security Studies* (pp. 511–533). Springer International Publishing. https://doi.org/10.1007/978-3-031-41574-6_27
33. *OptimaBank*. (2024). https://www.optimabank.kg/index.php?option=com_content&view=article&id=5010:attention-there-was-a-phishing-page-in-order-to-steal-funds-from-cards&catid=4&lang=ru&Itemid=110
34. Paul Joseph, D., & Norman, J. (2020). A Review and Analysis of Ransomware Using Memory Forensics and Its Tools. In S. C. Satapathy, V. Bhateja, J. R. Mohanty, & S. K. Udgata (Eds.), *Smart Intelligent Computing and Applications* (Vol. 159, pp. 505–514). Springer Singapore. https://doi.org/10.1007/978-981-13-9282-5_48
35. Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. Automated cybersecurity anti-phishing techniques. *Computer Science Review*, *29*, 44–55.
36. Quisumbing, L. A. (2017). Global Perspectives on Cyber security Using Latent Dirichlet Allocation Algorithm. *International Journal of Applied Engineering Research*, *12*(20), 10310–10323.
37. Ramazhamba, P. T., & Venter, H. S. (2023). Using distributed ledger technology for digital forensic investigation purposes on tendering projects. *International Journal of Information Technology*, *15*(3), 1255–1274. https://doi.org/10.1007/s41870-023-01215-9
38. Sangwan, S. (2022). A REVIEW ON CYBER CRIME PREVENTION USING STEGANOGRAPHY. *International Journal for Research Publication and Seminar*, *13*(1), 176–181. https://jrps.shodhsagar.com/index.php/j/article/view/226
39. Scanlon, M., Breitinger, F., Hargreaves, C., Hilgert, J.-N., & Sheppard, J. (2023). ChatGPT for digital forensic investigation: The good, the bad, and the unknown. *Forensic Science International: Digital Investigation*, *46*, 301609. https://doi.org/10.1016/j.fsidi.2023.301609
40. Scanlon, M., Nikkel, B., & Geradts, Z. (2023). Digital forensic investigation in the age of ChatGPT. *Forensic Science International: Digital Investigation*, *44*,. https://forensicsandsecurity.com/papers/ChatGPT.php
41. Schwarz, K., & Creutzburg, R. (2021). Design of professional laboratory exercises for effective state-of-the-Art OSINT investigation tools-Part 3: Maltego. *Electronic Imaging*, *33*, 1–23.
42. Semko, M., & Krakhmalyov, O. (2023). Electronic information as evidence. *Вестник Национального Технического Университета "ХПИ."* https://doi.org/10.20998/2227-6890.2021.1.07
43. Seo, S., Seok, B., & Lee, C. (2023). Digital forensic investigation framework for the metaverse. *The Journal of Supercomputing*, *79*(9), 9467–9485. https://doi.org/10.1007/s11227-023-05045-1
44. Serebrennikova, A. V., & Serebrennikova, M. S. (2021). Criminological innovations in criminality prevention: Status and perspectives. *SHS Web of Conferences*, *108*, 03002. https://www.shs-conferences.org/articles/shsconf/abs/2021/19/shsconf_blf2021_03002/shsconf_blf2021_03002.html
45. Singh, C., Tara, H., & Mishra, A. (2022). Digital Evidence Collection. In *Manual of Crime Scene Investigation* (pp. 145–156). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003129554-9/digital-evidence-collection-chintan-singh-harshita-tara-amarnath-mishra
46. Singh, S., & Kumar, S. (2020). Qualitative Assessment of Digital Forensic Tools. *Asian J. Electr. Sci*, *9*(1), 25–32.

47. Sumadinata, W. S. (2023). CYBERCRIME AND GLOBAL SECURITY THREATS: A CHALLENGE IN INTERNATIONAL LAW. *Russian Law Journal*, *11*(3), 438–444.
48. Tomer, S., Apurva, A., Ranakoti, P., Yadav, S., & Roy, N. R. (2017). Data recovery in Forensics. *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, 188–192. https://ieeexplore.ieee.org/abstract/document/8284474/
49. Tudosi, A.-D., Balan, D. G., & Potorac, A. D. (2022). New Snort rule for detection and prevention of SMTP e-mail bomb attacks. *2022 International Conference on Development and Application Systems (DAS)*, 78–84. https://ieeexplore.ieee.org/abstract/document/9786213/
50. van der Kleij, R., Wijn, R., & Hof, T. (2020). An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. *Computers & Security*, *97*, 101970.
51. Verma, A., & Shri, C. (2022). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision: The Journal of Business Perspective*, 097226292210747. https://doi.org/10.1177/09722629221074760
52. Winter, C., & Gundur, R. V. (2024). Challenges in gaining ethical approval for sensitive digital social science studies. *International Journal of Social Research Methodology*, *27*(1), 31–46. https://doi.org/10.1080/13645579.2022.2122226
53. Приколотина, Ю. Л. (2022). Проблемы и возможности криминологических исследований в условиях преобразующейся реальности. *Вестник Полоцкого Государственного Университета. Серия D. Экономические и Юридические Науки*, *12*, 152–157.
54. Серебренникова, А. В. (2020). Криминологические проблемы цифрового мира (Цифровая криминология). *Всероссийский Криминологический Журнал*, *14*(3), 423–430.