https://doi.org/10.31891/2219-9365-2024-78-43
УДК 621.3:004.6

ЛОЗОВСЬКИЙ Ростислав
https://orcid.org/0009-0004-9611-9424
e-mail: rawrshah@gmail.com
МОРОЗ Антон
https://orcid.org/0009-0001-1942-8432
e-mail: airmoroz26@gmail.com
ДАРМОГРАЙ Давид
https://orcid.org/0009-0001-7315-3353
e-mail: d.darmohrai@gmail.com

КІБЕРБЕЗПЕКА: ПРОБЛЕМИ, ВИКЛИКИ ТА МОЖЛИВІ РІШЕННЯ

Надійна і захищена робота мереж передачі даних, комп'ютерних систем і мобільних пристроїв є критично важливою для функціонування держави і забезпечення економічної стабільності суспільства. Безпека роботи ключових інформаційних систем, які використовуються широким колом користувачів, залежить від безлічі факторів, таких як кібер-атаки, фізичні порушення, збої в програмному та апаратному забезпеченні, а також людські помилки. Ці проблеми чітко показують, наскільки сучасне суспільство залежить від стабільності інформаційних систем. Кожен з цих факторів може спричинити серйозні наслідки для функціонування критичних інфраструктур, від енергетичних систем до фінансових установ. Тому забезпечення безпеки інформаційних систем є не лише технічним завданням, а й важливою складовою загальної національної безпеки. Важливо також враховувати, що нові загрози постійно еволюціонують, що вимагає постійного оновлення та вдосконалення систем захисту. Окрім традиційних підходів до кібербезпеки, необхідно впроваджувати інноваційні рішення і технології, які можуть допомогти виявляти і реагувати на нові види загроз. Таким чином, ефективна кібербезпека є запорукою не лише стабільності держави, а й загального добробуту суспільства.

Ключові слова: мережа, кібербезпека, інформаційна безпека, загрози.

LOZOVSKYI Rostyslav, MOROZ Anton, DARMOHRAI Davyd

CYBERSECURITY: ISSUES, CHALLENGES, AND POSSIBLE SOLUTIONS

Reliable and secure operation of data transmission networks, computer systems, and mobile devices is critically important for the functioning of the state and ensuring the economic stability of society. The security of key information systems, used by a wide range of users, depends on numerous factors such as cyber-attacks, physical disruptions, software and hardware failures, and human errors. These issues clearly demonstrate how modern society depends on the stability of information systems. Each of these factors can have serious consequences for the operation of critical infrastructures, from energy systems to financial institutions. Therefore, ensuring the security of information systems is not only a technical task but also a crucial component of overall national security. It is also important to recognize that new threats are constantly evolving, which requires continuous updating and improvement of protection systems. In addition to traditional approaches to cybersecurity, it is necessary to implement innovative solutions and technologies that can help detect and respond to new types of threats. Thus, effective cybersecurity is key not only to the stability of the state but also to the overall well-being of society.

Keywords: network, cyber security, information security, threats.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Кібербезпека все частіше розглядається як стратегічна проблема держави, яка комплексно зачіпає економіку країни, включно з взаємодією національних розробників програмного забезпечення і систем управління, виробників обладнання та компонентів для забезпечення ІКТ-інфраструктури. Низька ринкова конкурентоспроможність цих виробників призводить до необхідності використовувати рішення іноземних виробників. На практиці це явище спричиняє швидке зростання залежності від іноземних виробників і зниження рівня інформаційної безпеки через вимушене використання "закритого" програмного та апаратного забезпечення у всіх сегментах інфраструктури, як у спеціальних державних відомствах, так і в цивільному секторі.

Вже найближчим часом залежність від іноземних виробників обладнання та розробників програмного забезпечення може досягти критичного рівня. Наприклад, незважаючи на створену віртуальну "залізну завісу", влада Китаю фактично визнала повну залежність і незахищеність через повсюдне використання програмної платформи для мобільних пристроїв Android (частка платформи на ринку Китаю за підсумками 2012 року становила 86,4%), що базується на "відкритому" коді, але підконтрольна спеціальним службам США. З точки зору економіки, це явище має позитивний вплив на розвиток електронної промисловості та реального сектора, які використовують "відкрите" програмне забезпечення для виробництва мобільних пристроїв, але при цьому створює реальну загрозу для національної безпеки, переводячи її під контроль іноземних спецслужб.

ISSN 2219-9365

Для того щоб національна кібербезпека відповідала рівню провідних економічних держав, потрібні послідовні дії з боку держави, спрямовані на підвищення ефективності та розвиток системи взаємодії учасників ІКТ-галузі.

У свою чергу, підприємства-розробники та виробники повинні приділяти особливу увагу питанням інформаційної безпеки у своїй продукції, висуваючи підвищені вимоги до надійності та захищеності запропонованих рішень. Тільки в крайніх випадках і за необхідності підвищення ринкової орієнтованості окремих продуктів можна використовувати рішення іноземних постачальників та розробників програмного забезпечення.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Слід зазначити, що різні теоретичні та практичні аспекти кібербезпеки вже активно досліджуються як в Україні, так і за кордоном. Наприклад, технічні деталі та особливості захисту інформаційних систем розглядалися О. Неретіним і В. Харченком, В. Савченком і О. Шаповаленко, а також І. Стьопочкіною і О. Новіковим. Перспективи розвитку методів кіберзахисту для ефективного реагування на нові та змінені кіберзагрози були проаналізовані С. Шаровим. Огляд міжнародних ініціатив у сфері законодавчого регулювання кібербезпеки здійснив С. Цяпа. В закордонній науковій літературі роль і потенціал сучасних технологій у кібербезпеці, а також можливі напрямки їх подальшого розвитку досліджували Т. Сіпола, Р. Мостіна, Р. Дас і Р. Сандхейн.

Проте, незважаючи на значний обсяг досліджень, залишаються відкритими питання щодо практичної інтеграції нових методів і технологій у національні системи кібербезпеки. Це включає ефективну взаємодію між різними компонентами системи безпеки, етичні і правові аспекти захисту даних та забезпечення прозорості у прийнятті рішень. Важливими є також питання стійкості до атак та збоїв систем кіберзахисту, а також інтеграція нових технологій у вже існуючу інфраструктуру безпеки як на національному, так і на міжнародному рівнях.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є: визначити ключові напрями для покращення кібербезпеки, включаючи необхідність модернізації інфраструктури, розвитку кваліфікованих кадрів, впровадження нових технологій і стратегій захисту.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Поняття кібербезпеки охоплює безліч проблем різного типу, а також містить ще більше рішень. Кібербезпека є сферою активних досліджень та розробок у спільноті інформаційних технологій, що здійснюються учасниками з усіх частин екосистеми ІКТ.

Багато напрямів кібербезпеки мають спільні теми та проблеми, які потребують комплексного підходу. В табл. 1 коротко виділені деякі з основних проблем кібербезпеки, а також показано, де деякі з цих проблем вдається вирішувати за допомогою технічних рішень, розроблених комерційними організаціями, організаціями зі стандартизації та користувачами Інтернету.

Таблиця1

Проблеми кібербезпеки та технологічні рішення

Проблеми кібербезпеки	Технологічні рішення
Шкідливе програмне забезпечення (віруси, черв'яки)	Антивірусні програми, системи виявлення вторгнень (IDS)
Троянські коні	Антивірусне програмне забезпечення, моніторинг системної активності
Бот-мережі	Фільтрація трафіку, системи виявлення бот-мереж
Фішинг	Антифішингові фільтри, навчання користувачів
DDoS-атаки (розподілені атаки типу «відмова в обслуговуванні»)	Системи захисту від DDoS, мережеві брандмауери
Атаки «людина посередині»	Шифрування даних, використання VPN, протоколи безпечної передачі даних (HTTPS, TLS)
Уразливості в програмному забезпеченні	Регулярне оновлення програмного забезпечення, використання безпечних практик розробки коду
Неавторизований доступ до даних	Використання багатофакторної автентифікації, контроль доступу
Витік даних	Шифрування даних, політики управління даними, моніторинг доступу
Соціальна інженерія	Навчання користувачів, контроль доступу, впровадження політик безпеки

У переважній більшості випадків найуспішніші атаки хакерів, злочинців та інших зловмисників спрямовані на сервери та комп'ютери кінцевих користувачів, підключені до Інтернету. Серед інструментів, які використовуються для атак на комп'ютери, – шкідливе ПЗ, троянські коні, бот-мережі, фішинг, розподілені атаки типу «відмова в обслуговуванні» (DDoS), а також атаки «людина посередині».

Таблиця 2

Приклади спеціалізацій світових компаній у сфері інформаційної безпеки

Назва компанії	Країна походження	Спеціалізація	Опис спеціалізації
Cisco Systems	США	Мережева безпека	Розробка рішень для захисту корпоративних мереж, фаєрволи, VPN, системи виявлення загроз
Palo Alto Networks	США	Системи виявлення вторгнень, фаєрволи	Розробка апаратних та програмних рішень для захисту від кіберзагроз на рівні мережі
Check Point	Ізраїль	Брандмауери, системи виявлення загроз	Пропозиція комплексних рішень для мережевої безпеки, захисту даних та запобігання загроз
Symantec (NortonLifeLock)	США	Антивірусне програмне забезпечення, захист кінцевих точок	Захист персональних комп'ютерів, мобільних пристроїв, виявлення та видалення шкідливого програмного забезпечення
McAfee	США	Антивірусне ПЗ, безпека кінцевих точок	Розробка рішень для захисту домашніх і корпоративних користувачів від шкідливих програм, вірусів та кіберзагроз
FireEye	США	Розслідування кіберінцидентів, захист від просунутих загроз	Пропозиція рішень для виявлення та реагування на кіберзагрози, розслідування інцидентів
Trend Micro	Японія	Антивірусне ПЗ, безпека хмарних середовищ	Розробка рішень для захисту даних у хмарних середовищах, захист кінцевих точок, запобігання вторгненням
Fortinet	США	Мережева безпека, брандмауери, VPN	Пропозиція рішень для захисту корпоративних мереж, віртуальних приватних мереж, виявлення та запобігання загроз
IBM Security	США	Безпека великих даних, кіберзахист, аналітика	Розробка рішень для моніторингу безпеки, управління подіями безпеки, аналітика великих даних для виявлення загроз
Sophos	Велика Британія	Захист кінцевих точок, шифрування даних	Пропозиція комплексних рішень для захисту від шкідливих програм, шифрування даних, мережевої безпеки
CrowdStrike	США	Захист кінцевих точок, виявлення та реагування на загрози	Розробка хмарних рішень для моніторингу та захисту кінцевих точок, виявлення та реагування на кіберзагрози
F-Secure	Фінляндія	Антивірусне ПЗ, безпека хмарних середовищ, захист кінцевих точок	Пропозиція рішень для кіберзахисту, захисту даних у хмарних середовищах, виявлення та запобігання шкідливим програмам

Забезпечення безпеки комп'ютерів, будь то сервери, настільні комп'ютери, ноутбуки чи смартфони, є метою роботи різних груп всередині IT- та Інтернет-спільнот. Таблиця 2 допоможе визначити деяких великих гравців, а також області їхніх інтересів. Важливо зазначити, що переважна більшість компаній, представлених у таблиці, – це іноземні розробники та виробники, які здебільшого домінують на українському ринку.

Однак навіть наявність технологічного рішення для проблеми кібербезпеки не означає, що сама проблема зникає — просто з'являється можливість її вирішення. Наприклад, комплексне шифрування з використанням алгоритмів SSL/TLS є добре відомою технологією, яку можна використовувати для вирішення багатьох проблем, зазначених вище. Проте вона не була прийнята повсюдно. Частково це пояснюється історичними причинами та організаційною інертністю, а також низькою грамотністю або поганою поінформованістю. Наявність добре відомих рішень для добре відомих проблем має незначну цінність, якщо ці рішення не використовуються.

Таким чином, питання забезпечення національної кібербезпеки залежать не лише від технічних способів реалізації, але, що більш важливо, від наявності та реального попиту на ці рішення.

У програмах розвитку кібербезпеки уряди багатьох країн приділяють особливу увагу інфраструктурі, тісно пов'язаній з питаннями безпеки. Для оцінки масштабу проблем кібербезпеки та можливих загроз важливо розуміти взаємозв'язок між кібербезпекою, критичною інфраструктурою (CI), критичною інформаційною інфраструктурою (CII), захистом критичної інформаційної інфраструктури (CIIP) та інфраструктурою, що не є критичною. Цей взаємозв'язок представлений у таблиці 3.

Хоча визначення можуть дещо відрізнятися, критичною інфраструктурою (CI) зазвичай вважаються ключові системи, послуги та функції, несправність або руйнування яких має негативний вплив на систему охорони громадського здоров'я та безпеки, комерційну діяльність, національну безпеку або їхнє поєднання. CI складається як з матеріальних (наприклад, будівлі та споруди), так і з віртуальних елементів (наприклад, систем і даних). Кожна країна може мати своє розуміння терміну «критичний», однак зазвичай це поняття може включати елементи інформаційно-комунікаційних технологій (ІКТ) (включаючи телекомунікації, енергетику, банківську справу, транспорт, охорону здоров'я, сільське господарство та продовольство, водопостачання, хімічну промисловість, судноплавство, а також важливі державні служби).

Таблиця 3

Зв'язок між кібербезпекою та захистом критичної інформаційної інфраструктури

Аспект	Кібербезпека	Захист критичної інформаційної інфраструктури (CIIP)
Мета	Захист від кіберзагроз, забезпечення конфіденційності, цілісності та доступності інформації	Захист ключових систем та інформаційних активів, що мають критичне значення для національної безпеки
Об'єкти захисту	Сервери, мережі, кінцеві пристрої, дані	Інформаційні системи, мережі, телекомунікації, управлінські системи, які підтримують критичні сектори
Загрози	Шкідливе ПЗ, віруси, фішинг, DDoS-атаки, атаки на цілісність даних, атаки типу «людина посередині»	Цілеспрямовані атаки на критичні об'єкти, саботаж, кібершпигунство, маніпуляція даними
Технологічні рішення	Антивірусні програми, фаєрволи, шифрування, багатофакторна автентифікація, VPN	Комплексні системи моніторингу, захисту та реагування на інциденти, фізичний захист об'єктів
Учасники	IT-фахівці, спеціалісти з кібербезпеки, користувачі	Державні агентства, спеціалізовані відомства, оператори критичних інфраструктур, національні серти
Правові та нормативні акти	Стандарти ISO/IEC 27001, GDPR, NIST Cybersecurity Framework	Національні та міжнародні стандарти, закони про захист критичної інфраструктури, директиви ЄС
Вплив порушення безпеки	Втрата даних, компрометація особистої інформації, фінансові збитки, пошкодження репутації	Загроза національній безпеці, порушення функціонування суспільно важливих систем, загроза громадському здоров'ю

Кожен із цих секторів економіки має свої власні матеріальні ресурси, такі як будівлі банків, електростанції, поїзди, лікарні та урядові офіси. Водночас усі ці критичні сектори національної економіки залежать від інформаційно-комунікаційних технологій.

Кібербезпека в Україні стала важливою складовою національної безпеки через зростання кіберзагроз і атак. У сучасному світі, де інформаційні технології проникають у всі сфери життя, критична інфраструктура країни, така як енергетичні системи, транспортні мережі та державні установи, піддається значним ризикам. Проблеми в цій сфері проявляються через численні загрози, зокрема атаки на критичні системи, збільшення кількості шкідливого програмного забезпечення і зниження рівня кіберграмотності серед населення.

Україна стикається з викликами, такими як необхідність адаптації до швидко змінюваного кіберсередовища, яке постійно вдосконалюється, а також геополітичними напруженнями, що спричиняють кібервійни і політичні атаки. Інтеграція нових технологій у системи кібербезпеки є ще одним важливим викликом, з яким потрібно боротися.

Економічні наслідки кібератак, включаючи фінансові втрати і пошкодження репутації, також становлять серйозну загрозу. Внаслідок атак виникають витрати на відновлення і можливі збитки через крадіжки даних. Важливо також враховувати негативний вплив на довіру споживачів і бізнесів.

Для вирішення цих проблем Україні потрібно розвивати національну стратегію кібербезпеки, зокрема створюючи комплексні програми захисту та підвищуючи рівень координації між державними органами. Важливим аспектом є також підвищення рівня освіти та підготовки кадрів у сфері кібербезпеки, що включає розробку навчальних програм і інвестування у підготовку спеціалістів.

Необхідно також збільшити фінансування для проектів кібербезпеки, залучаючи як державні, так і приватні інвестиції, а також розвивати інноваційні технології для захисту інформаційних систем. Удосконалення законодавства та нормативної бази, зокрема актуалізація законів та посилення міжнародної співпраці, є ще одним важливим кроком для забезпечення національної кібербезпеки.

Таким чином, кібербезпека в Україні потребує комплексного підходу, що включає адаптацію до нових загроз, розвиток інфраструктури, підвищення освіти та кваліфікації фахівців, а також удосконалення правової бази та міжнародної співпраці.

Повномасштабна агресія росії проти України внесла безліч унікальних викликів, зокрема атаки на фізичну інфраструктуру, проблеми з людськими ресурсами та значне збільшення кіберзагроз. Частина цих викликів була передбачуваною, проте деякі вимагали тривалого часу для адаптації та стабілізації.

На початковому етапі війни однією з головних проблем стала невизначеність і необхідність швидкого прийняття рішень. Невідомість щодо подальшого розвитку ситуації вимагала підготовки до різних сценаріїв і швидкої адаптації до нових умов.

Серед найбільш критичних і неочікуваних викликів були ракетні атаки на важливу інфраструктуру, таку як електричні мережі та телекомунікації. В умовах цих атак виникли проблеми з доступом до даних і ресурсів. Обмеження на використання хмарних сервісів, запроваджені до початку війни, ускладнили процеси зберігання і обробки даних. Після скасування обмежень стало пріоритетом створення резервних копій систем у хмарі, що дозволило забезпечити стійкість та оперативність у роботі.

Незважаючи на те, що IT-інфраструктура може бути розміщена в хмарі, а персонал працювати віддалено, для ефективної роботи необхідно мати надійний зв'язок, стабільне енергозабезпечення та кінцеві пристрої. Забезпечення цих аспектів є критично важливим для підтримання функціонування систем кібербезпеки.

Перші місяці війни були ознаменовані швидкими змінами і адаптацією. Західні компанії надавали безкоштовні ліцензії та послуги, і виникла необхідність в обміні запасними частинами та обладнанням між організаціями. Були створені резервні канали зв'язку і супутниковий інтернет для забезпечення безперервної роботи.

Однією з головних проблем залишалася недостатня кількість кваліфікованих кадрів. Зростання кіберризиків призвело до підвищеного попиту на спеціалістів у галузі кібербезпеки, що ускладнило ситуацію на ринку праці. Проте автоматизація процесів і підготовка нових спеціалістів дозволили адаптуватися до нових умов.

Сучасні кіберзагрози включають DDoS-атаки, сканування вразливостей та фішинг. У 2022 році було зафіксовано збільшення кількості кібератак, хоча з початку 2023 року їх частота зменшилася. Попри зменшення атак, важливо продовжувати посилення кібербезпеки і підтримку ефективних систем захисту в умовах постійних загроз.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Кібербезпека є критично важливою складовою сучасної національної безпеки, особливо в умовах постійного зростання кіберзагроз. Постійна еволюція атакуючих методів і технологій вимагає від держав та організацій гнучкості і швидкого реагування на нові виклики. Оскільки цифрові технології проникають у всі сфери життя, атаки на критичну інфраструктуру, такі як енергетичні системи, транспортні мережі та державні установи, стають серйозними загрозами.

Однією з головних проблем є невизначеність, з якою стикаються організації на початкових етапах кризових ситуацій. Швидкість змін і непередбачуваність подій вимагають чіткої і гнучкої стратегії для управління ризиками та забезпечення оперативного реагування на загрози.

Модернізація інфраструктури стає необхідною для забезпечення ефективного захисту. Інвестиції у хмарні рішення та резервні системи є важливими для підвищення стійкості до атак. Водночас наявність надійного зв'язку, стабільного енергозабезпечення і відповідного обладнання є основою для підтримки функціонування інформаційних систем у кризових умовах.

Кіберзагрози також підкреслюють важливість кваліфікованих кадрів. Нехватка спеціалістів у сфері кібербезпеки може стати суттєвим бар'єром для ефективного захисту систем. Адаптація до нових умов, автоматизація процесів і підготовка нових фахівців є ключовими аспектами для подолання цього виклику.

Економічні наслідки кіберзагроз, включаючи фінансові втрати і репутаційні ризики, ще більше акцентують потребу в інвестиціях у кібербезпеку. Витрати на відновлення після атак та збитки від крадіжки даних демонструють важливість постійного вдосконалення заходів захисту.

Комплексний підхід до кібербезпеки, що включає національні стратегії і міжнародну співпрацю, є необхідним для забезпечення надійного захисту інформаційних систем. Оновлення законодавства, вдосконалення стандартів і розвиток міжнародних партнерств можуть суттєво підвищити рівень захисту в сучасному цифровому середовищі. Таким чином, кібербезпека потребує постійного вдосконалення і адаптації, щоб ефективно справлятися з новими загрозами та викликами.

Література

1. Неретін О., Харченко В. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. Information Systems And Networks. 2022. № 12. С. 7-20.

2. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. Сучасний захист інформації. 2020. № 4 (44). С. 6-11.

3. Стьопочкіна І.В., Новіков О.М. Методи штучного інтелекту в кібербезпеці: навч. посіб. для здобувачів спец. 125 “Кібербезпека”. Київ: КПІ ім. Ігоря Сікорського, 2022. 82 с.

4. Шаров С.В. Сучасний стан розвитку штучного інтелекту та напрямки його використання: зб. наук. пр. Інноваційні обрії України. 2023. № 6. С.136-144. – (Громадська організація Українські студії в європейському контексті).

5. Цяпа С.М. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій штучного інтелекту в сучасних умовах. Інформація і право. № 2(37)/2021. С. 51-59.

6. Tuomo Sipola, Tero Kokknen, Mika Karjalainen Artificial Intelligence and Cybersecurity: Theory and Applications. JAMK University of Applied Sciences. Publisher: Springer; 1st ed. 2023 edition (December 8, 2022). 311 p. DOI 10.1007/978-3-031-15030-2

7. Narcisa Roxana Mosteanu. Artifical Inelligence and cyber security – face to face with cyber attack – a maltese case of risk management approach. Ecoforum journal. 2020. Vol 9. № 2. URL: http://www.ecoforumjournal.ro/index.php/eco/article/view/1059

8. Rammanohar Das, Raghav Sandhane. Artificial Intelligence in Cyber Security. ICACSE 2020. IOP

Publishing. Journal of Physics: Conference Series 1964 (2021). P.1-10 doi:10.1088/1742-6596/1964/4/042072. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072/pdf

9. Гладка Ю.А., Назаренко Є.О. Аналіз застосування технологій штучного інтелекту в кібербезпеці: наукові праці третьої Міжнар. наук.-практ. конф. Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій, м. Київ, 25 – 26 січня 2021 р. Київ: НУХТ, 2021. С. 64-66.

10. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.20 р. № 1556 URL: https://zakon.rada.gov.ua/laws/show/ 1556-2020-p#Text

11. Про затвердження Плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021 – 2024 роки: Розпорядження Кабінету Міністрів України від 12.05.21 р. № 438 URL: https://zakon.rada.gov.ua/laws/show/438-2021-p#Text

12. Федоров: в Україні став доступний чат-бот зі штучним інтелектом ChatGPT. – (Українські національні новини від 18.02.23 р.). URL: https://www.unn.com.ua/uk/news/20160 33-fedorov-v-ukrayini-stav-dostupniy-chat-bot-zi-shtuchnim-intelektom-chatgpt

13. ChatGPT. The impact of Large Language Models on Law Enforcement. Europol Public Information. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20Enforcement.pdf

14. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682.

15. Givi BEDIANASHVILI, Hanna ZHOSAN, Sergiy LAVRENKO Modern digitalization trends of Georgia and Ukraine. Published in Scientific Papers. Series "Management, Economic Engineering in Agriculture and rural development", Vol. 22 ISSUE 3, 2022 https://managementjournal.usamv.ro/index.php/scientific-papers/current

16. Yankovoi, R., Stadniichuk, R., Zhosan, H., Garafonova, O., Biriukov, I. INNOVATIVE TRANSFORMATION OF A FINANCIAL INSTITUTION IN THE CONTEXT OF DIGITALISATION AND ITS IMPACT ON SOCIAL CONFLICT MANAGEMENT Financial and Credit Activity: Problems of Theory and PracticeThis link is disabled., 2024, 2(55), pp. 75–88 DOI: 10.55643/fcaptp.2.55.2024.4386

References

1. Neretin, O., & Kharchenko, V. (2022). Ensuring cybersecurity for artificial intelligence systems: Analysis of vulnerabilities, attacks, and countermeasures. Information Systems and Networks, 12, 7-20.

2. Savchenko, V. A., & Shapovalienko, O. D. (2020). Main directions of applying artificial intelligence technologies in cybersecurity. Modern Information Protection, 4(44), 6-11.

3. Stiopochkina, I. V., & Novikov, O. M. (2022). Methods of artificial intelligence in cybersecurity: A textbook for students of specialty 125 “Cybersecurity”. Kyiv: KPI named after Igor Sikorsky.

4. Sharov, S. V. (2023). Current state of artificial intelligence development and its application directions. Innovative Horizons of Ukraine, 6, 136-144.

5. Tsapa, S. M. (2021). Review of foreign legislative initiatives for the strategic use of artificial intelligence technologies in modern conditions. Information and Law, 2(37), 51-59.

6. Sipola, T., Kokknen, T., & Karjalainen, M. (2022). Artificial Intelligence and Cybersecurity: Theory and Applications. Springer. https://doi.org/10.1007/978-3-031-15030-2

7. Mosteanu, N. R. (2020). Artificial Intelligence and Cybersecurity – Face to Face with Cyber Attack – A Maltese Case of Risk Management Approach. Ecoforum Journal, 9(2). http://www.ecoforumjournal.ro/index.php/eco/article/view/1059

8. Das, R., & Sandhane, R. (2021). Artificial Intelligence in Cyber Security. Journal of Physics: Conference Series, 1964, 1-10. https://doi.org/10.1088/1742-6596/1964/4/042072

9. Hladka, Y. A., & Nazarenko, Y. O. (2021). Analysis of the use of artificial intelligence technologies in cybersecurity. In Proceedings of the Third International Scientific and Practical Conference on Modern Trends in the Development of Information Systems and Telecommunication Technologies (pp. 64-66). Kyiv: NUHT.

10. Cabinet of Ministers of Ukraine. (2020). On Approval of the Concept for the Development of Artificial Intelligence in Ukraine: Order of December 2, 2020, No. 1556. https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text

11. Cabinet of Ministers of Ukraine. (2021). On Approval of the Action Plan for Implementing the Concept for the Development of Artificial Intelligence in Ukraine for 2021–2024: Order of May 12, 2021, No. 438. https://zakon.rada.gov.ua/laws/show/438-2021-p#Text

12. Ukrainian National News. (2023). Fedorov: A Chatbot with Artificial Intelligence ChatGPT is now available in Ukraine. https://www.unn.com.ua/uk/news/2016033-fedorov-v-ukrayini-stav-dostupniy-chat-bot-zi-shtuchnim-intelektom-chatgpt

13. Europol. (n.d.). ChatGPT: The Impact of Large Language Models on Law Enforcement. https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20Enforcement.pdf

14. European Commission. (2021). Europe Fit for the Digital Age: Commission Proposes New Rules and Actions for Excellence and Trust in Artificial Intelligence. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

15. Givi BEDIANASHVILI, Hanna ZHOSAN, Sergiy LAVRENKO Modern digitalization trends of Georgia and Ukraine. Published in Scientific Papers. Series "Management, Economic Engineering in Agriculture and rural development", Vol. 22 ISSUE 3, 2022 https://managementjournal.usamv.ro/index.php/scientific-papers/current

16. Yankovoi, R., Stadniichuk, R., Zhosan, H., Garafonova, O., Biriukov, I. INNOVATIVE TRANSFORMATION OF A FINANCIAL INSTITUTION IN THE CONTEXT OF DIGITALISATION AND ITS IMPACT ON SOCIAL CONFLICT MANAGEMENT Financial and Credit Activity: Problems of Theory and PracticeThis link is disabled., 2024, 2(55), pp. 75–88 DOI: 10.55643/fcaptp.2.55.2024.4386