Наукові записки Львівського університету бізнесу та права.
Серія економічна. Серія юридична. Випуск 38/2023

http://dx.doi.org/10.5281/zenodo.10012434

Михальченко Г. Г.
доктор економічних наук, професор,
завідувач кафедри економіки підприємств та менеджменту,
Навчально-науковий професійно-педагогічний інститут,
Українська інженерно-педагогічна академія,
https://orcid.org/0000-0003-2616-9499

Снітко Ю. М.
старший викладач, кафедра правознавства та фінансів,
Полтавський інститут економіки і права
Відкритого міжнародного університету розвитку людини «Україна»,
https://orcid.org/0009-0002-7115-3867

Іваненко В. О.
кандидат економічних наук, доцент,
кафедра економіки, менеджменту, маркетингу та готельно-ресторанної справи,
соціально-психологічний факультет,
Житомирський державний університет імені Івана Франка,
https://orcid.org/0000-0003-2231-8485

КІБЕРБЕЗПЕКА В ЕКОНОМІЦІ: ЗАХИСТ ВІД КІБЕРЗАГРОЗ У ДИДЖИТАЛІЗОВАНОМУ СВІТІ

JEL Classification: G22
SECTION "ECONOMICS": Економіка

Анотація. Дослідження дало чітке розуміння того, що з цифровою трансформацією розвиваються засоби зламу мережевих систем. В дослідженні було проаналізовано закордонне та українське законодавство в сфері кібербезпеки. Виявлено, що в сучасному цифровому вимірі криптографія та платформи штучного інтелекту є рушійною силою в боротьбі з несанкціонованими мережевими вторгненнями. Доведено, що компанії, які приділяють достатню увагу та виділяють фінансові ресурси для захисту власних даних і даних клієнтів, менше ризикують зазнати фінансових втрат, а отже, є більш привабливими та конкурентоспроможними для клієнтів.

Ключові слова: диджиталізований світ, кібербезпека в економіці, кіберзахист, кіберзлочини, криптографія, штучний інтелект.

Annotation. The issue of data protection in today's digital society has become particularly acute due to the rapid proliferation of various network services in social and economic activities. Research indicates that methods for compromising network systems are advancing in tandem with digital transformation. During the study, a brief overview of cybersecurity legislation in other countries was conducted, and the legislation of Ukraine on the subject under investigation was analyzed in more detail. It was also demonstrated that since 2016, Ukraine has made cybersecurity one of the priorities in its national security framework. In particular, in 2017, another law was passed that regulates cybersecurity issues in Ukraine, further distinguishing between the concepts of cybersecurity and cyber defense. The most common methods of protection against cyberattacks in the corporate sector were identified and systematized. In the modern digital dimension, cryptography and artificial intelligence-based platforms have proven

to be driving forces against unauthorized network intrusions. The article proposes some general principles that can help enhance the effectiveness of encryption methods in combating cyber threats. It is demonstrated that artificial intelligence can determine the most effective data protection strategies, track viruses and malware, and create data recovery algorithms after cyberattacks. According to the research, companies that pay sufficient attention and allocate resources to safeguarding their own data and the data of their clients are at lower risk of suffering financial losses. Companies with a reliable security platform for their data are more attractive to clients and, consequently, more competitive.

Keywords: digital world, cybersecurity in economics, cyber defense, cybercrimes, cryptography, artificial intelligence.

Вступ

Сьогодні використання цифрових технологій не має жодних кордонів. Віртуальний простір домінує в усіх сферах людського життя. Національні світові економіки, банківські системи, транспортні та комунікаційні системи безпосередньо пов'язані з мережевими системами. У цьому контексті цифровий простір став привабливим для кіберзлочинців. Наразі все, що потрібно для скоєння злочину, — це відповідні навички та комп'ютер, підключений до мережі. Потенційними жертвами таких злочинців можуть бути як пересічні громадяни, так і вся критично важлива інфраструктура та економіка країни. Відтак, проблема кіберзлочинності є глобальною. Тому питання кібербезпеки та кіберзахисту в сучасному цифровому економічному просторі потребують подальших наукових досліджень.

Оскільки кіберзлочинність є основною проблемою сучасного суспільства, як політична, так і наукова спільноти шукають способи захисту від цієї епідемії, що стрімко поширюється. Так, Ю. Кінзерський приділяє особливу увагу дослідженню кібербезпеки в сучасній цифровій економіці [6]; В. Столбовий і Д. Кисленко [12] у своїх наукових дослідженнях розробляють питання кібербезпеки як у бізнес-, так і в державному секторах. В. Богом'я та В. Кочегаров [2] оцінювали криптографічні методи боротьби з кіберзлочинцями; Ю. Онищенко, О. Каланча і С. Гельдт [7] досліджували використання штучного інтелекту у сфері кібербезпеки. Однак через стрімку цифрову трансформацію тема кібербезпеки залишається актуальною і завжди потребує додаткових досліджень, оскільки кіберзлочинці адаптуються до новостворених систем захисту та знаходять нові способи здійснення кібератак.

Тому *метою* цього дослідження є оцінювання нормативно-правової бази з питань кібербезпеки в Україні та аналіз основних інструментів захисту від цифрових загроз у диджиталізованому світі.

Результати

Сучасна економічна сфера тісно пов'язана з цифровою трансформацією. Комп'ютерні технології полегшили доступ до таких побутових послуг, як оплата та купівля товарів, а також до освітніх послуг. Цифрові технології розширили можливості організації робочих процесів, насамперед завдяки електронній пошті, телефонним додаткам і комп'ютерному програмному забезпеченню для організації робочих процесів. Дійсно, інформаційні технології є одним із чинників нового способу життя, що ґрунтується на таких фундаментальних технологіях, як «Хмарні обчислення» («Cloud computing»), «Великі дані» («Big data»), та «інтернет речей» («Internet of Things»). Ці технології розширюють можливості опрацювання, збору, зберігання та аналізу великих обсягів даних, які успішно використовуються в різних бізнес-процесах, прискорюючи ухвалення стратегічних рішень і зменшуючи, а іноді й усуваючи ризик суб'єктивного негативного впливу людини [6].

Диджиталізація світу, а особливо диджиталізація виробничих процесів, є ключем до успішних бізнес-процесів. В сучасному суспільстві успішність неможлива без інновацій, а інновації не можуть здійснюватися без імпровізації. Потрібно зазначити, що в цьому контексті національний кіберпростір

визначає цифрове середовище економіки, основу електронних послуг і створює складне середовище, яке не може безпечно функціонувати без надійного захисту. Потрібно зазначити, що цифрова економіка зробила стрімкий крок уперед під час пандемії COVID-19. Саме завдяки попереднім напрацюванням щодо дистанційних функцій в організації бізнес-процесів дали змогу продовжити роботу та адаптуватися до нових економічних викликів. Водночас громадяни дедалі частіше дістають доступ до безпечних цифрових платформ і додатків, яким вони довіряють. Тому уряд і бізнес-сектор несуть відповідальність за розвиток і підтримку можливостей кібербезпеки, які гарантують безпечне використання цифрових послуг. Стрімка цифрова трансформація в різних галузях соціального та економічного життя не лише полегшила його, а й створила нові загрози, які раніше не були відомими, наприклад, ризик неправомірного використання та розповсюдження конфіденційної інформації про юридичних осіб та особистої інформації про фізичних осіб. З огляду на це, питання захисту цифрових даних постає особливо гостро і, беручи до уваги їхню розповсюдженість, відповідальність лежить на державі та бізнес-секторі, який надає послуги через цифрові сервіси [5; 12].

Приватні компанії часто стають жертвами кіберзлочинців, які активно використовують фішинг, мережеві атаки на рівні застосунків, мережеве сканування, веб-атаки, DDoS-атаки та розповсюдження шкідливого програмного забезпечення. Основною метою такої діяльності є отримання даних для незаконного збагачення [6].

Кібербезпека — це мінливе явище, оскільки кіберзлочинці постійно знаходять нові слабкі місця в програмному забезпеченні. Глобальний розвиток інтернету речей (IoT) зумовив поширення кіберзлочинності. Це пов’язано з тим, що все більше і більше пристроїв під’єднуються до інтернету і, як наслідок, кожен із цих пристроїв є потенційно вразливим до кібератак. Тому обмін інформацією між національними компаніями, установами, організаціями та урядами особливо важливий. Такий обмін інформацією може допомогти ефективніше виявляти кіберзагрози та обмінюватися набутим досвідом. Багато країн ухвалили законодавство про кібербезпеку. Наприклад, у Європі діє Загальний регламент про захист даних (GDPR), який встановлює вимоги до конфіденційності та захисту даних. В США питання захисту цифрових даних регулюється Законом про обмін інформацією про кібербезпеку (CISA), який регламентує комунікацію між бізнесом та урядом з питань кібербезпеки [13].

Україна активно займається питаннями кібербезпеки з 2016 року, з прийняттям Стратегії кібербезпеки України, затвердженої Указом Президента України № 96 від 15 березня 2016 року [9]. Відповідно до цієї стратегії було ухвалено Закон України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України» [8]. Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, передбачає повноваження державних органів, підприємств, установ, організацій, деяких осіб та громадян у цій сфері; встановлює основні засади координації діяльності у сфері кібербезпеки.

Отже, з 2017 року питання кібербезпеки в Україні врегульовано на законодавчому рівні. Хоча поняття кіберзахисту та кібербезпеки часто ототожнюють, законодавство чітко розмежовує їх.

Зокрема, кібербезпека в розумінні ст. 1 вказаного закону — це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, забезпечення сталого розвитку інформаційного суспільства та цифрового комунікаційного середовища, своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі. Кіберзахист — це комплекс організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їхніх наслідків та відновлення стійкості й надійності функціонування комунікаційних і технічних систем.

Як вбачається з вищесказаного, кібербезпека та її предмет має ширший і переважно теоретичний вимір. Водночас кіберзахист є вузькоспеціалізованим поняттям, в основі якого лежать технічні заходи з подолання кіберзагроз.

Загалом, Стратегію кібербезпеки України 2016 року було успішно реалізовано, і в таблиці 1 показано основні досягнення, здобуті за п'ять років реалізації стратегії.

Таблиця 1

Досягнення Стратегії 2016 р.	Питання кібербезпеки та кіберзахисту критичної інформаційної інфраструктури врегульовано на законодавчому рівні.
	Центри (підрозділи) кібербезпеки та кіберзахисту були створені в секторі безпеки та організаціях критичної інфраструктури, включно з Національним банком України, Службою спеціального зв'язку та захисту інформації України, Службою безпеки України, Міністерством оборони України, Міністерством інфраструктури України та Збройними силами України.
	Впроваджено систему виявлення вразливостей і реагування на кіберінциденти та кібератаки.
	Створена та діє урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.
	Створено Національний центр резервного копіювання національних інформаційних ресурсів.
	Національний координаційний центр кібербезпеки було створено для координації діяльності органів сектору безпеки та оборони, що забезпечують кібербезпеку.
	Посилено міжнародне співробітництво зі США, Великою Британією, Ірландією, Німеччиною, Нідерландами та Японією. Покращено співпрацю з ЄС і НАТО. Проведено кібернавчання за участю інших держав і міжнародних організацій.

Джерело: розроблення автора на основі [10].

Водночас досвід антитерористичної операції на сході України поставив пріоритети в цій сфері на перший план, оскільки атаки на критично важливу інфраструктуру України посилилися. Росія, зокрема, почала розвивати наступальні можливості кіберзброї. Кібератаки держави-агресора спрямовані на інформаційно-комунікаційні системи українських державних установ та об'єкти критичної інформаційної інфраструктури. Метою таких атак є прихований доступ, контроль або навіть виведення з ладу цифрового простору для ведення шпигунської або підривної діяльності. Такі кібератаки також негативно впливають на економіку країни загалом, оскільки в кіберпросторі здійснюється багато взаємопов'язаних процесів. Крім того, атаки на критичну інфраструктуру, чи то банківську, чи енергетичну, завжди мають прямий негативний вплив на бізнес-процеси. За таких обставин 26 серпня 2021 року було ухвалено нову Стратегію кібербезпеки № 447/2021. Як і в попередній стратегії, кібербезпека залишається одним із пріоритетів у системі національної безпеки України. Однак особлива увага приділяється загрозам з боку агресивного сусіда [10].

Світова спільнота цифрових експертів постійно шукає способи захисту від компрометації мережевих систем. Можна назвати найпоширеніші інструменти захисту, доступні для організацій від кіберзагроз. Особливо в поєднанні з оновленням програмного забезпечення, такі інструменти можуть значно підвищити рівень кібербезпеки та запобігти багатьом кібератакам, наприклад:

Фаєрволи. Програмне забезпечення, яке здійснює контроль вхідних і вихідних мережевих з'єднань. Саме фаєрволи захищають від зовнішніх атак і несанкціонованого витоку конфіденційної інформації.

Антивіруси. Програми, які виявляють і видаляють віруси і троянські програми.

Системи виявлення вторгнень. Такі системи виявляють потенційні ризики вторгнення в системи і, зокрема, фіксують нетипові дії в комп'ютерних мережах. Крім того, такі системи допомагають виявити потенційні вразливості в мережевих пристроях і програмному забезпеченні.

Криптографія або системи шифрування. Шифрування даних під час передавання в мережу гарантує конфіденційність даних та їх використання третіми особами.

Безпечні паролі. Найпростіший спосіб захистити дані — використовувати унікальні паролі. Паролі захищають користувачів від доступу третіх осіб до їхніх даних [3].

Шифрування — це зовсім інша справа, адже воно, фактично, запобігає використанню даних неавторизованими користувачами. Також криптографія гарантує цілісність даних і, зокрема, запобігає їхній підробці. Криптографія широко використовується, особливо в онлайн-банкінгу, електронній пошті, захисті інформації електронної комерції та там, де інформація передається за допомогою іншого інтернет-трафіку. Оскільки криптографічні протоколи можуть ускладнити наміри кіберзлочинців, криптографія також може захистити інформаційні дані від втручання злочинців і запобігти кібератакам [1].

Протягом останніх років особливої популярності набули хмарні сервіси, які дають змогу користувачам зберігати й обробляти дані у віддалених дата-центрах. Такі сервіси позбавляють користувачів необхідності мати власні сервери та обладнання. Хоча сучасні компанії широко використовують хмарні сервіси, кожна галузь має свої унікальні ризики кібербезпеки, які необхідно враховувати. Наприклад, компанії, що надають фінансові послуги, можуть зберігати й обробляти фінансову інформацію про своїх клієнтів, і в цьому випадку кіберзахист означає захист від фішингу, захист від кібератак на банківські системи та дотримання вимог законодавства щодо захисту фінансових даних. У сфері охорони здоров'я конфіденційні дані пацієнтів перебувають під загрозою атаки. Завдяки криптографії можна захистити дані пацієнтів від несанкціонованого отримання та відновити їх у разі пошкодження або втрати [2].

На рисунку 1 наведено деякі загальні принципи, які допомагають підвищити ефективність використання криптографічних методів.

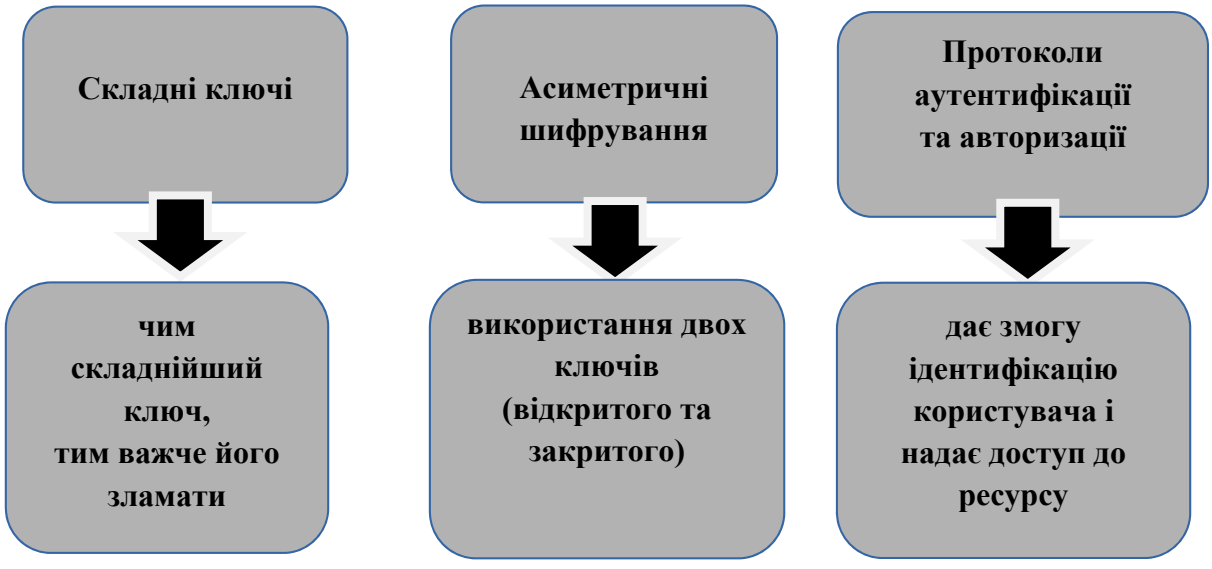

Рис. 1 Засоби підвищення ефективності криптографії

Джерело: розроблення авторів на основі [2].

Загалом, кібербезпека – це змінний процес, який потребує постійної гнучкості та адаптації, щоб цифрова трансформація не гальмувалась. Штучний інтелект (ШІ) – це інструмент, який може допомогти в боротьбі з кіберзлочинністю. Зокрема, ШІ може ідентифікувати потенційно небезпечні

типи програм, визначати найкращі стратегії захисту даних і створювати алгоритми для відновлення програм після хакерської атаки. Особливо ШІ може виявляти потенційні загрози, взаємодіяти з біометричними даними та втручатися в кіберінциденти. Загалом, штучний інтелект у сфері кібербезпеки є одним із найефективніших інструментів, які компанії можуть використовувати для зниження ризику кібератак. Зокрема, ШІ можна використовувати для відстеження нових вірусів, а також ШІ може виявляти небезпечне програмне забезпечення ефективніше і швидше, ніж людина [7; 11].

Наведені нижче платформи є актуальним розробленням на основі штучного інтелекту:

IBM QRadar Advisor with Watson. Застосунок, який здійснює розслідування повторюваних загроз центу безпеки.

IBM QRadar Incident Forensics. Додаток, за допомогою якого можливо відстежувати та аналізувати дії кіберзлочинців, що дає змогу усвідомити потенційні можливості зламу системи безпеки та відновити дані, пов'язані з інцидентом безпеки.

IBM QRadar Data Store. Платформа, яка використовує штучний інтелект для аналізу та зберігання великих обсягів даних, пов'язаних із безпекою та транзакціями.

IBM QRadar Data Synchronization App. Додаток, за допомогою якого можливо копіювати дані та файли і конфігурації. Такі можливості дають змогу відновити дані та файли в разі хакерських атак та інших ймовірних ризиків знищення інформації.

Balbix Security Cloud. Платформа для аналізу на основі штучного інтелекту з використанням камер спостереження. Це дає змогу прогнозувати ризики в режимі реального часу. Платформа допомагає експертам з кібербезпеки підтримувати системи в необхідному стані та запобігати іншим негативним наслідкам програм-вимагачів [7].

Метою розроблення вищезазначених платформ є захист даних, і компанії, які якнайшвидше розгортають автоматизовані рішення для гарантування безпеки, мають менший ризик втрат, ніж ті, що активно використовують новітні технології штучного інтелекту для запобігання кібервторгненням у свої мережеві системи. Деякі з переваг такого підходу перераховані нижче. Чим швидше програмне забезпечення виявляє ризик порушення або руйнування цілісності даних, тим нижча вартість відновлення даних, тому запобігати вторгненням вигідніше, ніж витрачати фінансові ресурси на виправлення порушень і відновлення даних [11].

Дослідження останнього десятиліття показують, що використання можливостей штучного інтелекту в боротьбі з кіберзагрозами зростає з кожним роком. Це пояснюється нестачею людських ресурсів і недоцільністю постійного повторного аналізу та виявлення загроз злому мережевих систем. Штучний інтелект посідає своє законне місце в цій галузі, оскільки він може миттєво виявляти кіберзагрози і перешкоджати потенційним вторгненням ще до того, як вони розпочнуться. Тому в сучасній цифровій економіці штучний інтелект є надійним способом захисту від кіберзагроз [7]. Бізнес, який прагне залишатися конкурентоспроможним в умовах цифрової економіки, має використовувати всі можливі інструменти для накопичення та оволодіння конкурентними перевагами, зокрема й інструменти кіберзахисту [4].

Тому автоматизація кіберзахисту є дієвим інструментом, який може зменшити ризики та потенційні збитки, спричинені можливими вторгненнями в мережеві системи. Нещодавні дослідження показали, що організації, які не використовують сучасні засоби захисту даних, вимушені зазнавати значних витрат на відновлення даних у майбутньому, і в результаті такі організації зазнають більших витрат, ніж ті, що інвестують фінансові ресурси в сучасний ефективний захист баз даних до того, як виникне потенційна кіберзагроза [11].

Висновки

Дослідження показує, що тема кібербезпеки наразі викликає значний інтерес як у наукових колах, так і на рівні національних урядів. Аналіз нормативно-правової бази захисту від кіберзагроз в Україні свідчить, що нині це питання розглядають у контексті захисту від кібератак з боку російської

федерації, яка з початком вторгнення на схід України у 2014 році активно вдається до мережевих систем нашої держави в пошуках вразливих та незахищених територій. Зрозуміло, що на це питання звертається особлива увага. У дослідженні було визначено способи захисту від кіберзагроз та окремо оцінено деякі з них. Зокрема, було виявлено, що штучний інтелект є однією з рушійних сил у боротьбі з кібератаками і в найближчому майбутньому він затьмарить людський потенціал у цій сфері. Сучасні технології кіберзахисту в сучасній цифровій економіці – це те, що визначає стабільність компаній та їхню конкурентоспроможність у сучасному, оцифрованому світі.

Водночас кіберзлочинність — явище мінливе, адаптивне та гнучке. З появою нових мережевих можливостей та інтернет-платформ з'являтимуться нові методи зламу та збору даних. Тому теми кібербезпеки та кіберзахисту залишатимуться актуальними й надалі. Однак особливу увагу потрібно приділити захисту мережевих систем об'єктів критичної інфраструктури в Україні.

Список використаних джерел

1. Борисова К. В. Світличний В. А. Використвння криптографії у боротьбі з кіберзлочинністю. П*ротидія кіберзлочинності та торгівлі людьми: з*бірн. Матер. Міжнар.наук.-прак. конф. м. Вінниця, 31 трав. 2023 р. Вінниця, 2023. С. 108 -109. URL : http://surl.li/kzwvy
2. Богом'я В. І., Кочегаров В. С. Кібербезпека в хмарних сервісах за допомогою застосування криптографічних методів. *Водний транспорт. Інформаційні технології.* Київ, 2023. № 1 (37). С 239-246. DOI : doi.org/10.33298/2226-8553.2023.1.37.27
3. Грищенко Д. О. Павленко С. М. Використання інформаційних технологій для захисту від основних видів кіберзлочинів. П*ротидія кіберзлочинності та торгівлі людьми:* збірник матеріалів Міжнар. наук.-практ. конф. м. Вінниця, 31 трав. 2023 р. Вінниця, 2023 113-114. http://surl.li/kzqmj
4. Зрибнєва І. П. Вироблення рішень щодо формування конкурентного потенціалу суб'єктів інноваційного підприємництва. Інтелект XXI. 2020. № 5. С. 150–155. URL : http://surl.li/kzxhs
5. Комова С. С. Пушкар Т. А. Кібербезпека в цифровій економіці. *Сталий розвиток міста:* матеріали XVI Всеукр. студ. наук.-техн. конф. м. Харків, 2023 р. Харків, ХНУМГ ім. О.М. Бекетова, 2023. С. 66 -68. URL : http://surl.li/hoauq
6. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки : проблеми взаємозв'язку. *Economics Bulletin*. 2020. №3. С. 18-26 https://doi.org/10.33271/ebdut/71.018
7. Онищенко Ю. М., Каланча А. А., Гельдт С. В. Застосування штучного інтелекту у сфері кібербезпеки. *Trends, theories and ways of improving science :* Proceedings of the VIII International Scientific and Practical Conference. Spain. Madrid, 2023, February 28 - March 03. С 544-547. URL : http://surl.li/kzqep
8. Про основні засади забезпечення кібербезпеки в Україні : Закон України від 05.10.2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text
9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. "Про Стратегію кібербезпеки України" : Указ Президента України від 15.03.2016 р. № 96/2016. URL : https://zakon.rada.gov.ua/laws/show/96/2016#n11
10. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text
11. Саєнко Д. О., Колісник Т. П. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Протидія кіберзлочинності та торгівлі людьми: з*бірн. Матер. Міжнар.наук.-прак. конф. м. Вінниця, 31 трав. 2023 р. Вінниця, 2023. С. 158-160. http://surl.li/kzqnc

12. Столбовий В. М. Кисленко Д. П. Заходи підвищення кібербезпеки на державному та корпоративному рівнях в умовах диджиталізації суспільства. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.* Львів, 2023. Випуск 37. С. 175-183. URL : http://surl.li/kzxct
13. Ширяєв Д. О. Кібербезпека та сучасний світ. *Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів :* тези доп. Всеукр. наук.-практ. конф. м. Вінниця, 17 травн. 2023 р. Вінниця, 2023. С. 600-602. URI **:** https://dspace.univd.edu.ua/handle/123456789/17602