Інформаційне право

УДК: 004.42

DOI https://doi.org/10.5281/zenodo.14757503

Безпека персональних даних в умовах війни: технології проти кіберзлочинців

Гунько Ольга Юріївна

директор компанії CyberField NeT, викладач IT, експерт у сфері кібербезпеки, (Україна, місто Вінниця)

Южека Роман Сергійович

аспірант навчальної групи АС-941 третього освітньо-наукового рівня вищої освіти «доктор філософії / Ph.D.» кафедри кримінально-правових дисциплін Навчально-наукового інституту права та інноваційної освіти Дніпровського державного університету внутрішніх справ, член Громадської організації «Спілка освітян України», ORCID ID: https://orcid.org/0009-0007-6031-4182, (Україна, місто Дніпро)

Прийнято: 14.01.2025|Опубліковано: 28.01.2025

Анотація. *У статті розглядаються проблеми забезпечення безпеки персональних даних в умовах війни, коли кіберзагрози набувають особливої актуальності через зростання кіберзлочинності. З розвитком інформаційних технологій та зростанням залежності від цифрових систем збільшується ризик кібератак, що може мати серйозні наслідки для конфіденційності, цілісності та доступності персональних даних. Особливу загрозу становлять атаки на критичну інфраструктуру, державні установи та приватні компанії, що в умовах війни може бути використано як засіб дестабілізації. З метою захисту даних в умовах постійних кіберзагроз використовуються методи шифрування,*

багаторівневий захист, системи виявлення вторгнень, а також інноваційні технології, такі як штучний інтелект та блокчейн. Особливу увагу приділено проблемам адаптації політик безпеки до вимог Регламенту ЄС (GDPR), а також необхідності міжнародної співпраці в боротьбі з кіберзлочинністю. Для підвищення ефективності захисту даних необхідно постійно вдосконалювати технології, розробляти нові підходи та проводити навчання користувачів і фахівців. Стаття також акцентує на важливості розвитку квантових технологій, штучного інтелекту та нових методів шифрування для боротьби з найсучаснішими кіберзагрозами.

Ключові слова: *безпека персональних даних, кібербезпека, війна, кіберзлочинці, захист даних, шифрування, багаторівневий захист, фішинг, рансомвар, машинне навчання, блокчейн, кіберзагрози, конфіденційність, національна безпека, цифрові технолог.*

Security of personal data in war conditions technologies against cybercriminals

Hunko Olha Yuriyivna

Director of CyberField NeT, IT Instructor, Expert in Cybersecurity, (Ukraine, Vinnytsia)

Yuzheka Roman Serhiyovych

PhD student of the AS-941 academic group Third educational-scientific level of higher education "Doctor of Philosophy / Ph.D." Department of Criminal Law Disciplines Educational and Scientific Institute of Law and Innovative Education Dniprovsk State University of Internal Affairs, Member of the Public Organization "Union of Educators of Ukraine", ORCID ID: https://orcid.org/0009-0007-6031-4182, (Ukraine, Dnipro)

Abstract. *The article addresses the issues of ensuring the security of personal data in wartime conditions, when cyber threats become particularly relevant due to the rise in cybercrime. With the development of information technologies and growing*

reliance on digital systems, the risk of cyberattacks increases, which can have serious consequences for the confidentiality, integrity, and availability of personal data. Particular threats include attacks on critical infrastructure, government institutions, and private companies, which in wartime may be used as a means of destabilization. To protect data in the context of ongoing cyber threats, methods such as encryption, multi-layered protection, intrusion detection systems, and innovative technologies like artificial intelligence and blockchain are used. The article also focuses on the challenges of adapting security policies to the requirements of the EU General Data Protection Regulation (GDPR), as well as the need for international cooperation in the fight against cybercrime. To enhance data protection effectiveness, it is necessary to continuously improve technologies, develop new approaches, and conduct user and specialist training. The article also emphasizes the importance of developing quantum technologies, artificial intelligence, and new encryption methods to counter the most advanced cyber threats.

Keywords: *personal data security, cybersecurity, war, cybercriminals, data protection, encryption, multi-layered protection, phishing, ransomware, machine learning, blockchain, cyber threats, confidentiality, national security, digital technologies.*

Вступ. У сучасному світі інформаційні технології стали невід'ємною частиною повсякденного життя, що охоплює не лише бізнес, а й особисту сферу. Однак зі зростанням залежності від цифрових систем збільшується й ризик злочинної діяльності у кіберпросторі, зокрема в умовах війни. Військові конфлікти, як ніколи, підштовхують до активізації кіберзагроз, що можуть мати критичні наслідки для безпеки не лише державних структур, а й кожної окремої людини.

Кіберзлочинці, використовуючи уразливості цифрових технологій, можуть викрадати, маніпулювати або руйнувати особисті дані, що в умовах війни стає не тільки питанням приватності, а й національної безпеки. Водночас

розвиваються нові технології, які допомагають захистити дані, підвищити стійкість до атак та гарантувати безпеку в умовах постійних кіберзагроз.

Постановка проблеми. Безпека персональних даних в умовах війни є важливим аспектом для забезпечення конфіденційності, цілісності та доступності інформації. З огляду на підвищений ризик кібератак, захист даних вимагає комплексного підходу та використання різноманітних технологій, методів і стратегій для протидії кіберзлочинцям.

Матеріали для забезпечення безпеки персональних даних включають розроблені стандарти й норми, такі як Регламент ЄС про захист персональних даних (GDPR) і національні закони про кібербезпеку. Вони встановлюють вимоги щодо збору, зберігання та обробки персональних даних, а також обов'язки організацій щодо їх захисту [1].

Після набрання чинності Загальним регламентом про захист даних (далі – GDPR) чимало компаній зіткнулися з проблемою адаптації політики приватності до нових вимог у сфері захисту персональних даних. Ключові вимоги до змісту політики приватності містяться у статтях 13 і 14 GDPR. Основна помилка при складенні політики приватності – це розпорошення інформації про окрему обробку персональних даних серед різних розділів, коли укладачі описують категорії оброблюваних даних окремо від цілей, а цілі – окремо від правових підстав обробки (згода, інтерес, вимога закону тощо) [2, с. 228].

Методи забезпечення безпеки персональних даних включають використання шифрування для захисту даних під час передачі й зберігання. Системи багатофакторної аутентифікації допомагають запобігти несанкціонованому доступу до чутливої інформації. Важливими методами є також створення резервних копій даних, що дозволяє відновити інформацію у разі її втрати внаслідок кібератак.

В умовах війни зростає актуальність кіберзахисту інфраструктури, зокрема критичної, яка може бути піддана кібератакам з боку ворога. Це включає впровадження систем моніторингу і виявлення аномальних дій, а також

оперативне реагування на кіберзагрози, зокрема через аналіз і блокування шкідливих програм, атак на мережу або інші системи.

Технології, що використовуються для протидії кіберзлочинцям, включають засоби виявлення вторгнень, системи захисту від вірусів та шкідливих програм, а також технології машинного навчання і штучного інтелекту для автоматичного виявлення нових загроз. Також застосовуються методи криптографії для забезпечення захищеного зв'язку і конфіденційності даних.

Таким чином, для ефективної безпеки персональних даних в умовах війни необхідне постійне вдосконалення технологій і методів захисту, а також навчання користувачів і фахівців для швидкої адаптації до нових кіберзагроз.

Аналіз останніх досліджень і публікацій. Безпека персональних даних є однією з найбільш актуальних тем у сфері кібербезпеки, особливо в умовах війни. Кіберзлочинці використовують різні методи для здійснення атак на інформаційні системи, що має серйозні наслідки для конфіденційності та захисту персональних даних. Останні дослідження у цій галузі підкреслюють важливість застосування новітніх технологій для боротьби з кіберзлочинцями, особливо в контексті збройних конфліктів.

Питання боротьби з кіберзлочинністю розглядалися багатьма науковцями. Зазначеним питанням приділяли увагу такі дослідники як О.М. Бандурка, В.В. Василевич, В.В. Голіна, Б.М. Головкін, А. П. Закалюк, О.М. Литвинов, В.В. Марков, В.І. Трапезніков, В.О. Туляков, І. В. Жук, Я. В. Левківська та інші. Аналіз правового регулювання персональних даних у Європейському Союзі став предметом численних наукових досліджень. Зокрема, І. Сопілко [3, с. 75] досліджував міжнародно-правовий досвід захисту персональних даних. Проблему відповідності українського законодавства європейським стандартам у цій сфері вивчали М. Бем, І. Городиський [4, с. 255], М. Різак [5, с. 72], О. Легка [6, с. 79] та інші науковці. І. Брацук та І. Яворська аналізували практику судів ЄС щодо принципів захисту персональних даних у контексті європейського правового поля [7, с. 198]. Проте, у сфері безпеки персональних даних в умовах

війни залишається ряд невирішених проблем, що потребують додаткових досліджень. Зокрема, це включає удосконалення алгоритмів шифрування для забезпечення надійності захисту в умовах високих кіберзагроз, розробку нових підходів до виявлення та нейтралізації аномальних дій з використанням штучного інтелекту, а також інтеграцію квантових технологій для захисту даних від потенційних майбутніх атак. Крім того, необхідно вирішити питання міжнародної співпраці в боротьбі з кіберзлочинністю, яка стає все більш глобальною, та забезпечити адекватне правове регулювання застосування штучного інтелекту, що включає визначення чітких норм щодо обробки персональних даних і захисту приватності. Важливою є також потреба в постійному удосконаленні підходів до навчання користувачів та фахівців для швидкої адаптації до нових кіберзагроз і викликів, що виникають унаслідок збройних конфліктів.

Виділення невирішених раніше частин загальної проблеми. У період війни загроза з боку кіберзлочинців значно зростає, оскільки зростає кількість кібератак на державні, комерційні та приватні системи. Ці атаки можуть включати фішинг, інфікування комп'ютерних мереж шкідливим програмним забезпеченням, а також атаки на інфраструктуру зв'язку, що є критично важливим для збереження стабільності країни в умовах війни. Для того, щоб протистояти таким загрозам, вчені та фахівці з кібербезпеки активно розробляють і впроваджують нові технології для захисту персональних даних.

Серед основних підходів до забезпечення безпеки даних в умовах війни є шифрування, багаторівневий захист, використання систем виявлення та запобігання вторгненням, а також технології блокчейн для зберігання та захисту інформації. Шифрування є одним із найбільш ефективних засобів захисту даних, оскільки воно дозволяє запобігти несанкціонованому доступу до інформації навіть у випадку витоку даних. Разом з тим, важливим аспектом є використання технологій для виявлення і нейтралізації шкідливих програм, які можуть бути використані для крадіжки або зміни персональних даних.

Дослідження також показують, що в умовах війни особливу увагу слід приділяти захисту критичних інфраструктур, таких як електронні реєстри, системи управління урядом та інформаційні платформи, що забезпечують комунікацію між громадянами та державними органами. Це вимагає інтеграції новітніх технологій в інфраструктуру кібербезпеки, таких як системи штучного інтелекту для автоматичного виявлення аномальних дій в мережах та блокування потенційних загроз.

Загалом, останні дослідження вказують на необхідність постійного удосконалення технологій для забезпечення безпеки персональних даних в умовах війни. Сучасні технології та інновації в галузі кібербезпеки, такі як шифрування, штучний інтелект, системи виявлення вторгнень і блокчейн, допомагають підвищити рівень захисту та знизити вразливість до кіберзлочинців.

Формулювання цілей статті. Метою цієї статті є вивчення та аналіз технологічних і правових підходів до забезпечення безпеки персональних даних в умовах війни. У роботі зроблено акцент на важливості використання новітніх технологій, таких як шифрування, штучний інтелект і блокчейн, для підвищення рівня захисту даних від кіберзлочинців. Крім того, розглянуто необхідність інтеграції міжнародного співробітництва у боротьбі з кіберзагрозами, що стає важливою складовою ефективної стратегії кібербезпеки. В статті також висвітлено проблеми правового регулювання обробки персональних даних та необхідність удосконалення національних законів з урахуванням міжнародних стандартів. Основним внеском є пропозиція інтеграції квантових технологій у захист даних як перспективного напрямку в боротьбі з кіберзлочинністю.

Виклад основного матеріалу дослідження. Безпека персональних даних в умовах війни є одним з найбільш важливих аспектів сучасної кібербезпеки. Війна створює додаткові загрози для інформаційних систем, оскільки кіберзлочинці та ворожі держави використовують новітні технології для досягнення своїх цілей, зокрема через атаки на критичні інфраструктури та виток персональних даних. Ці атаки можуть мати серйозні наслідки, включаючи

знищення або викрадення важливої інформації, порушення роботи державних установ, а також втрату довіри громадян до організацій.

Одним з основних методів, що використовуються кіберзлочинцями в умовах війни, є фішинг. Напади через фішинг спрямовані на обман користувачів з метою збору конфіденційної інформації, таких як паролі або фінансові дані. Крім того, рансомвар є ще одним популярним методом кібернападів, при якому зловмисники шифрують дані на заражених системах і вимагають викуп за їх розшифровку. Такі атаки можуть бути спрямовані як на приватні компанії, так і на державні установи, що має особливо серйозні наслідки в умовах війни, коли доступ до даних може бути критично важливим для стабільності держави.

Для протистояння цим загрозам використовуються різні технології, серед яких найбільш ефективними є методи шифрування даних, багаторівневий захист та використання систем виявлення та запобігання вторгненням. Шифрування даних є одним із найважливіших способів захисту, оскільки воно дозволяє забезпечити конфіденційність інформації навіть у випадку її викрадення. Багаторівневий захист передбачає використання різних технологій безпеки, таких як міжмережеві екрани, антивірусні програми та багатофакторну автентифікацію, що дозволяє знижувати ризик несанкціонованого доступу до інформаційних систем.

Використання штучного інтелекту для автоматичного виявлення загроз є однією з новітніх тенденцій у кібербезпеці. Інтелектуальні системи здатні оперативно аналізувати великі обсяги даних, виявляти аномалії в роботі системи та реагувати на загрози ще до того, як вони призведуть до серйозних наслідків.

Станом на сьогодні в Україні вже зроблені перші кроки для створення правового регулювання галузі штучного інтелекту. Ще у 2020 році була створена Концепція розвитку штучного інтелекту в Україні, в якій уперше на законодавчому рівні надається визначення, мета, принципи та завдання розвитку технологій штучного інтелекту в Україні [8].

Однією з останніх законодавчих ініціатив, які стосуються використання Штучного інтелекту в Україні є Законопроєкт №8153 «Про захист персональних даних» [9].

Метою розробки цього законопроєкту є приведення норм українського законодавства до міжнародних стандартів. Зокрема, в ньому деталізовано принципи обробки персональних даних, вимоги до згоди на обробку персональних даних, які забезпечують уникнення зловживаннями та маніпуляціями, визначено обов'язки контролерів та операторів персональних даних, а також запроваджено фінансову відповідальність та адміністративні санкції до контролера або оператора за порушення права на захист персональних даних.

Крім того, технології блокчейн, завдяки своїм властивостям незмінності та прозорості даних, можуть бути використані для зберігання важливої інформації, що значно ускладнює її викрадення чи зміну.

Невід'ємною частиною сучасної стратегії кіберзахисту є співпраця між державними структурами та приватними компаніями. Кіберзлочинці часто діють у складі міжнародних груп, тому координація дій на глобальному рівні є необхідною для ефективного захисту від загроз. Спільні зусилля урядів, корпорацій та міжнародних організацій дозволяють створювати комплексні рішення для боротьби з кіберзлочинністю, що включають обмін інформацією про загрози, розробку нових стандартів безпеки та реагування на кризові ситуації.

Проте перехід до новітніх технологій із застосуванням штучного інтелекту поміж численних переваг супроводжуються й значними ризиками. Недостатня конфіденційність особистих даних може призвести до порушень прав громадян, а тому питання впровадження технології штучного інтелекту вимагає якісного правого регулювання та впровадження ефективних механізмів захисту персональних даних від незаконної обробки, у тому числі від втрати, незаконного або випадкового знищення, а також від незаконного доступу до них сторонніх осіб [10].

Штучний інтелект чи окремі його елементи могли б бути використаними також зокрема для моніторингу способу життя, виявлення порушень, пов'язаних із конфліктом інтересів, порушень при одержанні подарунків, сумісництві та суміщенні посад. Так, штучний інтелект може аналізувати інформацію із соціальних мереж, використовувати алгоритми обробки тенденцій поведінки, аналізувати громадську думку та виявляти інші факти [11, с. 117-118].

Водночас використання описаних інструментів має національний характер, адже на сьогодні в Україні відсутня нормативно-правова база, яка б комплексно регулювала суспільні відносини, що виникають при застуванні штучного інтелекту, відтак це питання лише частково врегульовано Законом України «Про захист персональних даних» та Концепцією розвитку штучного інтелекту 2020 року [12, с. 123]. З метою правового закріплення штучного інтелекту в Україні планується масштабна співпраця з міжнародними організаціями та залучення європейського досвіду, зокрема в розробці стандартів захисту прав і свобод учасників таких відносин та Етичного кодексу використання штучного інтелекту [13]. У міжнародних актах, які мають суто рекомендаційний характер щодо характеристики штучного інтелекту, відображено принципи роботи зі штучним інтелектом у судових системах – Європейська етична хартія Ради Європи щодо використання штучного інтелекту в судових системах [14]. Також у цій сфері було створено Технічний комітет зі штучного інтелекту SC N 42 у рамках Міжнародної організації зі стандартизації, що розробляє практики, проєкти та доповіді [15]. Міжнародно-правове регулювання означеного аспекту суспільних відносин зосереджено у міжнародних актах, які мають суто рекомендаційний характер щодо характеристики штучного інтелекту.

Отже, забезпечення безпеки персональних даних в умовах війни вимагає використання передових технологій і інтегрованих підходів до захисту. Шифрування, багаторівневий захист, штучний інтелект, блокчейн та міжнародна співпраця є основними інструментами, що допомагають ефективно протистояти

кіберзлочинцям і зберігати конфіденційність даних у складних умовах сучасних конфліктів.

Висновки та подальші перспективи. У зв'язку зі швидким розвитком кіберзагроз та постійним вдосконаленням методів атак, безпека персональних даних в умовах війни залишається надзвичайно важливою проблемою, що потребує постійної уваги та інвестицій у новітні технології. Результати дослідження показують, що існуючі заходи захисту, такі як шифрування даних, багаторівневий захист і технології виявлення загроз, є ефективними, проте для боротьби з найскладнішими та адаптивними кіберзагрозами необхідно розвивати нові підходи.

Одним із важливих аспектів є необхідність постійного удосконалення алгоритмів шифрування та інтеграції новітніх технологій, таких як квантове шифрування, що здатне протистояти навіть найпотужнішим атакам. Квантові технології обіцяють кардинально змінити підхід до захисту даних, оскільки їх принципи безпеки базуються на законах квантової фізики, що забезпечують практично абсолютну надійність захисту.

У майбутньому великий потенціал для підвищення рівня безпеки персональних даних мають також штучний інтелект та машинне навчання. Вони можуть автоматично виявляти нові типи атак і адаптувати системи безпеки до змінюваних умов, що є критично важливим у періоди збройних конфліктів, коли кіберзлочинці постійно змінюють свої методи. Розвиток технологій виявлення аномалій на основі штучного інтелекту дозволить значно зменшити час реакції на загрози та забезпечити оперативний захист критичних систем.

Не менш важливим є і питання міжнародної співпраці в галузі кібербезпеки. В умовах глобалізації кіберзлочинність не має кордонів, і боротьба з нею вимагає координації між урядами, міжнародними організаціями та приватним сектором. Спільні зусилля у розробці стандартів безпеки, обміні інформацією про нові загрози та створенні ефективних механізмів реагування допоможуть посилити колективну оборону від кіберзлочинців та зменшити ризики для державних і приватних систем.

Подальші перспективи розвитку цієї галузі також пов’язані з підвищенням рівня обізнаності серед населення та державних структур щодо важливості захисту персональних даних. Залучення громадськості до питань кібербезпеки через освітні ініціативи та тренінги є важливим кроком у підготовці до протидії кіберзагрозам, адже часто саме людський фактор є слабким ланцюгом у системах безпеки.

Таким чином, забезпечення безпеки персональних даних в умовах війни вимагає комплексного підходу, що включає не тільки технологічні інновації, але й активну співпрацю між державними структурами, приватними компаніями та міжнародними партнерами. Використання новітніх технологій, постійний моніторинг та адаптація до нових викликів дозволять створити ефективну систему захисту даних, здатну витримати сучасні кіберзагрози.

Список використаних джерел

1. Європейський парламент та Рада Європейського Союзу. (2016). Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв’язку з обробкою персональних даних і про вільне переміщення таких даних (Загальний регламент про захист даних, GDPR). Офіційний журнал Європейського Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 06.01.2025).

2. Світличний В. А. Захист персональних даних в умовах воєнного стану в Україні. *Право і безпека.* 2023. № 3 (90). С . 226-236.

3. Сопілко І. М. Міжнародно-правовий досвід захисту персональних даних. *Юридичний вісник.* 2014. № 4. С. 70–75.

4. Бем М. В., Городиський І. М. Відповідальність за порушення законодавства про захист персональних даних: проблеми відповідності законодавства України вимогам регламенту Європейського Союзу щодо захисту персональних даних (GDPR). *Право України.* 2019. № 2. С. 237–255.

5. Різак М. В. Практика країн Європейського Союзу та України у сфері судочинства щодо гарантування безпеки обігу та обробки персональних даних. *Підприємство, господарство і право*. 2017. № 7. С. 68–72.

6. Легка О. В. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. *Правова позиція*. 2021. № 2. С. 74–79.

7. Брацук І. З., Яворська І. М. Практика Суду ЄС щодо принципів захисту персональних даних в ЄС. *Вісник Львівського університету*. 2019. № 47. С. 192–198.

8. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 06.01.2025).

9. Про захист персональних даних: проєкт Закону №8153 від 25.10.2022 р. URL: https://www.kmu.gov.ua/bills/proekt-zakonu-pro-zakhist-personalnikh-danikh (дата звернення: 06.01.2025).

10. У системі відеомоніторингу стану публічної безпеки запровадять єдині технічні та функціональні вимоги до відеоспостереження // Портал МВС: сайт. URL:https://mvs.gov.ua/news/u-sistemi-videomonitoringu-stanu-publicnoyibezpeki-zaprovadiat-jedini-texnicni-ta-funkcionalni-vimogi-do-videosposterezennia (дата звернення: 06.01.2025).

11. Миткалик С. І. Використання штучного інтелекту в роботі. Національного агентства з питань запобігання корупції. *ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВОВІЙ ПРАКТИЦІ: МЕЖІ ТА МОЖЛИВОСТІ : збірник тез Всеукраїнського круглого столу (15 березня 2024 року)* / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2024. 214 с. С. 115-119.

12. Тарасевич Т. Ю. Правове регулювання штучного інтелекту у сфері репродуктивних функцій людини: сучасні виклики та перспективи реалізацій. *Науковий вісник Ужгородського Національного Університету*. 2023. С. 123-130.

13. Токарєва К. С. Особливості правового регулювання штучного інтелекту в Україні. *Юридичний вісник*. 2021. № 3 (60). URL:

http://www.law.nau.edu.ua/images/Nauka/Naukovij_ jurnal/2021/3-60/23.pdf (дата звернення: 08.01.2025).

14. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018). URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c (viewed on 08.01.2025).

15. Artificial intelligence ISO/IEC JTC 1/SC 42. URL: https://www.iso.org/committee/6794475.html (дата звернення: 08.01.2025).