УДК 004.056.5 DOI: https://doi.org/10.32631/pb.2023.3.19

ВІТАЛІЙ АНАТОЛІЙОВИЧ СВІТЛИЧНИЙ,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0003-3381-3350,
e-mail: vit.svet@ukr.net

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Статтю присвячено проблемі захисту персональних даних в умовах воєнного стану в Україні. Проведено детальне дослідження цього питання, розглянуто аспекти нормативно-правового середовища та рівнів захисту персональних даних у таких складних умовах.
У контексті воєнного стану порушення конфіденційності персональних даних може створити серйозні загрози. Акцентовано увагу на тому, що розголошення таких даних може призвести до ризику для особистої безпеки людей, зокрема для учасників конфлікту. Це може стати основою для шантажу та маніпуляцій, що негативно впливає на становище окремих осіб і загальну ситуацію.
Надано рекомендації, спрямовані на запобігання таким загрозам та покращення рівня захисту персональних даних під час воєнного стану. Особливу увагу приділено необхідності розроблення та впровадження спеціалізованих нормативно-правових актів, які б регулювали захист персональних даних у таких надзвичайних ситуаціях. Також розглянуто можливості використання сучасних технологій, зокрема шифрування даних і багаторівневої аутентифікації, для підвищення безпеки та конфіденційності персональних даних.
Застосування ефективних заходів захисту персональних даних під час воєнного стану є важливим завданням для забезпечення безпеки та приватності людей. Додержання нормативно-правових вимог, розвиток технологій захисту даних і збільшення усвідомленості щодо цієї проблеми серед населення можуть сприяти зменшенню ризиків та збереженню конфіденційності персональних даних навіть в умовах воєнного конфлікту.
Висновки, представлені у статті, можуть стати цінним джерелом інформації для законодавців та фахівців з інформаційної безпеки, які займаються питаннями захисту персональних даних в умовах воєнного стану. Результати дослідження можуть сприяти розробленню та впровадженню ефективних стратегій захисту даних, спрямованих на забезпечення безпеки та приватності учасників конфлікту і громадян у цілому. Розглянуто важливі аспекти проблеми захисту персональних даних в умовах воєнного стану та надано рекомендації щодо покращення ситуації в цій галузі.

Ключові слова: *воєнний стан, захист персональних даних, кібербезпека, законодавство, приватність, державна безпека, шифрування, контроль доступу.*

Оригінальна стаття

ВСТУП. Мережа Інтернет є невід'ємною частиною життя багатьох українців. Підтвердженням цьому є інфографіка мультимедійної платформи іномовлення України – Укрінформ, згідно з якою кількість користувачів нерівномірно збільшується щороку (див. рис. 1)[1].

Враховуючи онлайн-активність українців, зокрема 82 % користувачів, що користувалися інтернетом у 2022 році хоча б на раз на тиждень, за даними Укрінформ, Державній службі спеціального зв'язку та захисту інформації України необхідно акцентувати увагу на вдосконаленні законодавства у сфері захисту персональних даних[2].

У контексті військового протистояння на сході країни та повномасштабної війни з росією інформаційна безпека набуває пріоритету. Дані Державної служби спеціального зв'язку

[1] В Україні кількість інтернет-користувачів зросла до 23 мільйонів // Укрінформ : сайт. 10.10.2019. URL: https://www.ukrinform.ua/rubric-technology/2797152-v-ukraini-kilkist-internetkoristuvaciv-zrosla-do-23-miljoniv.html (дата звернення: 15.08.2023).

[2] Близько 78 % українців сьогодні користуються інтернетом // Укрінформ : сайт. 01.06.2022. URL: https://www.ukrinform.ua/rubric-technology/3497671-blizko-78-ukrainciv-sodna-koristuutsa-internetom.html (дата звернення: 15.08.2023).

та захисту інформації України свідчать про зростання кібератак майже в 4 рази. Отже, стратегії захисту інформації виходять на перший план для національної безпеки. Аналіз дій України щодо захисту персональних даних у цих умовах визначає напрям нашого дослідження.

Рис. 1. Динаміка росту користувачів мережі Інтернет в Україні

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. *Метою* статті є детальний аналіз методів та засобів, які можуть бути застосовані для захисту персональних даних в умовах воєнного стану. Для досягнення максимальної ефективності та надійності захисту варто розглянути різні підходи і стратегії, які можуть бути використані в таких умовах.

Задля досягнення поставленої мети необхідно вирішити такі *завдання*: провести огляд літератури та проаналізувати наявні підходи до захисту персональних даних у воєнний час; вивчити законодавство щодо захисту персональних даних під час воєнних дій; проаналізувати ризики та загрози безпеці персональних даних в умовах воєнного стану; розглянути можливі підходи та стратегії для захисту персональних даних у воєнний час, враховуючи шифрування, захист мережі та інші методи; оцінити ефективність і надійність різних методів та засобів захисту персональних даних в умовах воєнного стану; розробити рекомендації щодо найкращих практик захисту персональних даних у воєнний час.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. У дослідженні використовувалися такі методи наукового пізнання, як аналіз, синтез, класифікація та порівняльний аналіз. Ці методи застосовувалися для вивчення ключових засобів захисту персональних даних в умовах воєнного стану, розгляду ефективних заходів щодо підвищення рівня кібербезпеки, а також для аналізу можливостей міжнародного співробітництва й обміну досвідом у сфері захисту персональних даних.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. Важливо зауважити, що захист персональних даних в умовах воєнного стану має бути пріоритетним завданням для держави, компаній та користувачів. Від цього залежить не лише інформаційна безпека держави та її громадян, а й їхні права та свободи.

Особливу увагу варто звернути на роль освіти та підвищення обізнаності користувачів у питаннях захисту персональних даних. Необхідно проводити різноманітні навчальні заходи та поширювати інформацію про можливі ризики та методи їх попередження. Це дозволить громадянам свідомо ставитись до збору та обробки їхніх персональних даних і допоможе зменшити кількість випадків їх незаконного використання.

Із початком широкомасштабного вторгнення в Україну значна кількість людей з-поміж іншої допомоги також потребує правового супроводу як на території України, так і за кордоном. За атрибуцією абсолютна більшість кіберінцидентів пов’язана з хакерськими угрупуваннями, що фінансуються урядом рф (Павлиш, 2022). Важливою умовою правомірної

обробки персональних даних у період дії правового режиму воєнного стану є забезпечення громадянам належного рівня захисту їхніх прав, пов'язаних із персональними даними.

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). Якщо проведений аналіз щодо персональних даних буде бездоганним, а людина залишається неуважною, це надасть іншим суб'єктам можливість соціального контролю (Сопілко, 2013, с. 65–66). Наприклад, на початку 2019 року Національна комісія з питань інформатизації і свободи Франції оштрафувала Google на 50 млн євро. Одним із порушень було те, що важлива інформація про цілі обробки, терміни зберігання категорій персональних даних, що підлягають обробці, була розміщена в різних документах. Французький регулятор зазначив, що Google не надає споживачам чіткої та доступної інформації про те, як саме збираються та зберігаються їхні персональні дані.

Загальні принципи захисту персональних даних – це набір основних положень та правил, яких повинні дотримуватися під час обробки та зберігання персональних даних. Ці принципи стосуються всіх суб'єктів обробки персональних даних, таких як компанії, урядові органи тощо.

До основних принципів захисту персональних даних належать такі.

1. Законність, добросовісність і прозорість. Цей принцип передбачає, що обробка персональних даних повинна здійснюватися відповідно до законодавства та відкрито для фізичних осіб, про яких зберігається інформація. Організації мають повідомляти про те, яку інформацію вони збирають, як вона використовується, кому передається та які права на захист персональних даних мають фізичні особи.

2. Мінімізація даних. Цей принцип вимагає, щоб обробка персональних даних здійснювалася лише в необхідному обсязі для досягнення визначених цілей. Організації повинні збирати та обробляти лише ту інформацію, яка необхідна їм для виконання своїх функцій, і не зберігати персональні дані довше необхідного часу.

3. Точність. Цей принцип передбачає, що персональні дані повинні бути точними й оновлюваними. Організації мають забезпечувати точність та актуальність персональних даних, а також гарантувати їхню своєчасну корекцію в разі необхідності.

4. Обмеження зберігання. Цей принцип вимагає, щоб персональні дані зберігалися тільки протягом часу, необхідного для досягнення цілей, для яких вони були зібрані. Після того, як дані стають непотрібними, їх потрібно видаляти або анонімізувати.

5. Інтегрітет даних і конфіденційність. Цей принцип передбачає, що персональні дані повинні бути захищені від несанкціонованого доступу, випадкової втрати або пошкодження. Організації повинні вживати всіх необхідних заходів для захисту персональних даних від несанкціонованого доступу, враховуючи шифрування та захист від злому.

6. Відповідальність. Важливість захисту персональних даних в умовах воєнного стану також зумовлена тим, що євроінтеграційні процеси України в цей час не стали «на паузу», а навпаки набрали ще більших обертів, тому стандартизація українського законодавства відповідно до норм та принципів європейського законодавства, а також вимог самого Європейського Союзу є надважливим аспектом розвитку нашої країни (Кравчук, 2022, с. 320).

Якщо порівняти з Європейським Союзом, то Україна має схожі принципи захисту персональних даних. В Україні діє Закон України «Про захист персональних даних», який має на меті захист прав і свобод громадян України від неправомірного використання їхніх персональних даних. Закон встановлює правила збору, зберігання, обробки та передачі персональних даних, а також відповідальність за їх неправомірне використання.

Однак Європейський Союз має більш суворі вимоги до захисту персональних даних. Зокрема, в ЄС було прийнято Загальний регламент про захист персональних даних (Бем, Городиський, 2018, с. 7–8), який набрав чинності 25 травня 2018 року. Цей Регламент встановлює єдині правила збору, зберігання, обробки та передачі персональних даних в ЄС, а також відповідальність за порушення правил їх захисту, за що можуть бути накладені великі штрафи аж до 20 млн євро, або 4 % річного обороту компанії.

Щодо відмінностей між принципами захисту персональних даних в Європейському

Союзі та Україні, то можна зауважити, що GDPR передбачає більш суворий контроль за захистом персональних даних, враховуючи необхідність отримання згоди на їх збір та обробку. Крім того, GDPR вимагає від компаній проводити оцінку впливу на захист персональних даних та повідомляти про порушення правил захисту персональних даних протягом 72 годин.

Закон України «Про захист персональних даних» також містить принципи захисту персональних даних, але він менш конкретний, ніж GDPR. Наприклад, Закон України «Про захист персональних даних» у своїх положеннях не визначає межі своєї дії в територіальному аспекті, а GDPR чітко визначає межі своєї територіальної юрисдикції. Крім того, в Україні немає такої ж суворої відповідальності за порушення правил захисту персональних даних.

Отже, хоча принципи захисту персональних даних в Європейському Союзі та Україні схожі, проте GDPR має більш суворий підхід до захисту персональних даних та встановлює жорсткіші вимоги до компаній щодо захисту персональних даних. Це вимагає від європейських підприємств збільшити свої зусилля у сфері захисту персональних даних, а також уважніше ставитися до вимог GDPR.

Підписавши Угоду про асоціацію з Європейським Союзом, Україна погодилась на співробітництво з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи, як це передбачено ст. 15 Угоди. Так, відповідно до ст. 11 Угоди про співробітництво між Україною та Європейською організацією з питань юстиції кожна її Сторона гарантує рівень захисту персональних даних, наданих іншою Стороною, принаймні еквівалентний тому, що випливає із застосування принципів, що містяться в Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року і наступних змін до неї, а також принципів, закладених у Рішенні щодо Євроюсту та в Регламенті Євроюсту щодо захисту даних (Рогова, 2011, с. 467).

Міжнародне співробітництво та обмін досвідом також здатні допомогти в підвищенні рівня захисту персональних даних. Україна може взяти на озброєння досвід Європейського Союзу щодо захисту персональних даних та використати його для покращення власних правил і підходів.

Отже, захист персональних даних є важливою та актуальною темою як в Європейському Союзі, так і в Україні. З метою забезпечення високого рівня захисту персональних даних необхідно запровадити комплекс заходів, які включають у себе: роз'яснення населенню ризиків використання персональних даних; підвищення кваліфікації фахівців; створення спеціалізованих підрозділів для захисту персональних даних; розробку та впровадження стратегії кібербезпеки, а також міжнародне співробітництво й обмін досвідом.

Під системою інформаційної безпеки країни зазвичай розуміють об'єднання органів державної влади, які виконують свої завдання на основі закону в умовах постійного контролю судової влади. Метою відповідної системи є: діагностика та прогнозування інформаційних загроз і ризиків, що впливають на стан життєво важливих інтересів суспільства; реалізація низки довготривалих заходів, спрямованих на попередження відповідних загроз; підтримка готовності до забезпечення інформаційної безпеки.

Фізичний захист об'єктів інформаційної інфраструктури (далі – ОІІ) є важливою складовою комплексу захисних заходів (Худолєй, Загребельна, 2023, с. 77–78). Він полягає в забезпеченні безпеки об'єктів, що містять інформацію, за допомогою різноманітних технічних, технологічних і організаційних заходів. Забезпечення фізичної безпеки ОІІ потребує запровадження комплексу заходів, які включають у себе захист приміщень, обладнання, транспорту, обробки й зберігання інформації, технічного забезпечення систем захисту інформації та інших складових. Свідченням цьому слугують слова Міністра внутрішніх справ І. Клименка, який заявив, що станом на лютий 2023 року порушено понад 80 тис. проваджень за фактами мародерства після початку повномасштабної війни. Із введенням воєнного стану, усі майнові злочини розглядаються як мародерство, зі збільшеним покаранням. Мародерство може відбуватися не лише стосовно матеріальних цінностей, але й стосовно майна, яке використовується для обробки персональних даних. Крім того, Міністр попереджає про можливе зростання кількості таких злочинів, оскільки багато людей повертаються в розграбовані домівки на деокупованих територіях[1]. Захист інформаційних систем і мереж

[1] За час воєнного стану в Україні порушили 80 тисяч справ через мародерство – Клименко // Слово і Діло : сайт. 09.02.2023. URL: https://www.slovoidilo.ua/2023/02/09/novyna/suspilstvo/chas-voyennoho-stanu-ukrayini-porushyly-80-tysyach-sprav-cherez-maroderstvo-klymenko (дата звернення: 26.03.2023).

передбачає застосування технічних та організаційних заходів для забезпечення безпеки інформації в комп'ютерних системах і мережах. Технічні заходи включають у себе захист мережі від несанкціонованого доступу, використання криптографії для захисту даних від перехоплення та забезпечення безпеки даних у хмарних сервісах; організаційні заходи – підвищення обізнаності персоналу щодо захисту інформації та встановлення політики щодо захисту інформації і процедур безпеки.

Основним компонентом фізичного захисту є безпека приміщень, де розміщене обладнання та системи інформаційної техніки. Для цього вживають технічних та організаційних заходів. Технічні заходи передбачають встановлення підвищених систем контролю доступу, антивандальних огороджень, камер відеоспостереження та розгортання воєнізованої охорони. Організаційні заходи зосереджені на адаптації правил інформаційної безпеки до умов воєнного стану, спеціальному навчанні персоналу й реагуванні на можливі загрози (Semchuk, 2023, p. 466). Додаткова увага приділяється захисту транспортних засобів, що перевозять обладнання інформаційної техніки, особливо в регіонах із підвищеною загрозою. Технічні заходи захисту транспорту включають у себе встановлення GPS-трекерів, антивандальних замків, сигналізації, а також заходи для забезпечення безпеки під час перевезення обладнання в умовах потенційних засідок або атак.

У воєнних умовах, які склалися в Україні, особливого значення набуває захист обробки й зберігання інформації як ключової частини фізичного захисту ОІІ. Серверні приміщення, дата-центри та інші об'єкти, де зберігається стратегічна інформація, потребують підсиленої уваги. Це передбачає встановлення систем контролю доступу, підвищених стандартів пожежної безпеки та систем виявлення вторгнень. Також критичною є потреба в технічному оснащенні систем захисту інформації. Це враховує використання спеціалізованого програмного забезпечення для захисту від кібератак, методів протидії злому паролів та інші заходи. Особливий акцент у воєнний час слід зробити на комбінованому підході до захисту ОІІ, що передбачає технічні, технологічні та організаційні заходи. Зокрема, це стосується безпеки персоналу, розробки процедур взаємодії в різних відділах організації та забезпечення безперебійної роботи систем. М. Бем та І. Городиський (2021, с. 105–106) наголошують, що вибір методів забезпечення безпеки персональних даних в умовах воєнного стану повинні ґрунтуватися на оцінці ризиків і з урахуванням проведеної оцінки актуальних і потенційних методів захисту. Також важливо дотримуватися вимог законодавства та нормативних актів у сфері інформаційної безпеки.

Отже, фізичний захист ОІІ є критично важливим у сучасних умовах, особливо в умовах воєнного стану в Україні. Він вимагає виваженого підходу, який охоплює технічні, технологічні та організаційні заходи. Фізичний захист враховує безпеку приміщень, обладнання, транспорту, обробку та зберігання інформації тощо. Правила інформаційної безпеки, навчання персоналу та реагування на надзвичайні ситуації також є важливими складовими цього процесу. Особливу увагу слід приділяти законодавчим вимогам та нормативам із питань інформаційної безпеки.

Кібербезпека та криптографічний захист даних також є важливими аспектами захисту персональних даних, оскільки зловмисники завжди прагнуть знайти способи доступу до особистої інформації користувачів.

Однією з основних складнощів для спецслужб та контррозвідки є не тільки збір інформації через розвідницькі операції, але й процес дезідентифікації зібраної інформації, шифрування конфіденційних джерел і приховання технічних джерел збору інформації. Важливо при цьому забезпечити доступність інформації для тих, хто потребує її для прийняття обґрунтованих рішень вчасно (Полтораков, 2014, с. 233).

Захист даних за допомогою криптографії забезпечує надійний рівень безпеки та зменшує ризики втрати конфіденційної інформації.

Для забезпечення кібербезпеки та криптографічного захисту даних користувачі повинні застосовувати надійний пароль та регулярно змінювати його, встановлювати оновлення програмного забезпечення, використовувати антивірусне програмне забезпечення та підписуватися на сервіси, які забезпечують безпеку даних.

Також важливо зауважити, що на рівні держав кібербезпека є важливою темою для урядів та організацій, які збирають, зберігають та обробляють персональні дані громадян. Уряди мають відповідати за безпеку персональних даних, які збираються під час реєстрації на різні державні послуги, використання банківських послуг та інших дій.

Для забезпечення кібербезпеки на державному рівні уряди запроваджують політику та різні правила забезпечення безпеки даних. Вони розробляють законодавство, що встановлює стандарти й правила захисту даних та передбачає відповідальність за їх порушення.

Використання персональних даних працівниками суб'єктів відносин, пов'язаних із персональними даними, повинно здійснюватися лише відповідно до їхніх професійних, службових або трудових обов'язків. Ці працівники зобов'язані не допускати розголошення в будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних, службових чи трудових обов'язків, крім випадків, передбачених законом. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом (Макушев, 2013, с. 333–334).

Криптографічний захист даних використовується також для захисту персональних даних на зберігання. Для цього послуговуються різними методами шифрування даних, як-от: AES (*Advanced Encryption Standard*), DES (*Data Encryption Standard*) та ін.

Отже, кібербезпека та криптографічний захист є важливими аспектами захисту персональних даних. Використання надійних методів захисту даних, таких як криптографічний, може значно зменшити ризики втрати конфіденційної інформації та захистити користувачів від кібератак. Крім того, на державному рівні важливо розробляти політику та законодавство, які забезпечують безпеку даних і накладають відповідальність за їх порушення.

При захисті персональних даних слід уживати різноманітних технічних та організаційних заходів. До них належать: встановлення надійних паролів, застосування двофакторної аутентифікації, використання криптографічних методів захисту даних, а також проведення аудитів та навчання користувачів з питань безпеки даних.

Крім того, важливо пам'ятати, що кібербезпека та криптографічний захист даних є напрямами, які постійно розвиваються. Необхідно регулярно оновлювати захисні програми та інструменти, а також використовувати останні версії протоколів захисту даних. Також варто стежити за новими загрозами та вчасно вживати заходів для їх запобігання.

У світі, де все більше інформації збирається та обробляється онлайн, захист персональних даних стає важливим завданням. Кібербезпека і криптографічний захист даних відіграють ключову роль у забезпеченні безпеки та конфіденційності даних. Якщо правильно використовувати захисні програми та інструменти, то можна значно зменшити ризики втрати конфіденційної інформації та забезпечити захист персональних даних (Джакомопулос, Буттарелі, О'Флаерті, 2018, с. 181–182).

Екстрені процедури реагування на інциденти також важливі для захисту персональних даних. Основна мета екстрених процедур реагування на інциденти полягає в тому, щоб мінімізувати їх наслідки та швидко відновити роботу системи. Це включає в себе виявлення, класифікацію, аналіз і вирішення проблеми. Швидке реагування може зменшити втрату даних, зберегти репутацію компанії та захистити від небажаних наслідків для користувачів.

При розробці екстрених процедур реагування на інциденти необхідно враховувати особливості конкретного бізнесу та об'єктів, що потребують захисту. Наприклад, важливо визначити пріоритетність обробки даних, що може допомогти забезпечити ефективне відновлення роботи системи та уникнення серйозних наслідків.

Крім того, необхідно проводити навчання персоналу щодо екстрених процедур реагування на інциденти. Це може допомогти збільшити ефективність захисних заходів та підвищити рівень свідомості з питань безпеки даних.

Оскільки інциденти можуть бути різного характеру, екстрені процедури реагування на них повинні бути гнучкими та адаптивними. Вони повинні бути орієнтовані на швидке виявлення проблеми та реагування на неї, а також на ефективність відновлення роботи системи і збереження даних.

Наступним важливим кроком у забезпеченні ефективності екстрених процедур є їх тестування та перевірка. Регулярне проведення тестів може допомогти виявити уразливість і потенційні проблеми, які можуть бути використані зловмисниками для здійснення кібератак. Крім того, тестування може допомогти виявити недоліки та помилки в екстрених процедурах і вчасно їх виправити.

З урахуванням зростання кількості кіберзлочинців, які цілять на доступ до персональних даних, такі процедури виявляються життєво необхідними для забезпечення конфіденційності та безпеки користувачів. Екстрені реакції на такі інциденти повинні бути негайними, щоб запобігти можливим втратам чи компрометації даних.

Важливо наголосити, що в умовах воєнного стану екстрені процедури реагування на інциденти мають бути під постійним контролем, адаптацією до поточної ситуації та регулярно піддаватися тестуванню. Своєчасність, точність та ефективність їх застосування може виявитися ключовим фактором у збереженні конфіденційної інформації. Навчання персоналу цим процедурам є обов'язковим,

адже підвищена освіченість у галузі безпеки даних може зменшити ризики злочинних втручань. Проте слід розуміти, що в умовах конфлікту екстрені процедури реагування на інциденти лише частина більшої системи захисту даних. Регулярний аналіз ризиків, оцінка захисних механізмів та адаптація до нових загроз є ключовими для гарантованого захисту персональних даних користувачів у складних умовах.

У світі, де все більше інформації збирається та обробляється в онлайн середовищі, екстрені процедури реагування на інциденти стають все важливішими. Вони дозволяють підтримувати безпеку даних та захищати їх від несанкціонованого доступу, а також забезпечують швидке відновлення роботи системи та мінімізацію наслідків інциденту. Тому при розробці стратегії захисту даних необхідно враховувати екстрені процедури реагування на інциденти та забезпечувати їх ефективність та адаптивність до нових загроз і викликів.

Кіберзлочинність у контексті воєнного конфлікту може бути використана як інструмент гібридної війни, спрямованої на дестабілізацію ситуації в країні. Тому стратегія захисту інформації повинна враховувати не лише традиційні методи, а й засоби протидії специфічним загрозам, характерним для воєнного стану (Блохін, 2022). Персональна інформація користувачів в умовах конфлікту може бути використана для розвідувальних цілей, дезінформаційних кампаній або навіть для безпосередніх атак. Тому крім традиційних методів захисту, таких як брандмауери чи антивірусні програми, може знадобитися спеціалізоване програмне забезпечення для криптографічного захисту даних і систем виявлення вторгнень.

Освіта і підготовка користувачів щодо потенційних загроз у воєнних умовах є ключовим елементом стратегії захисту. Особливо важливо навчати користувачів розпізнавати спроби соціальної інженерії та фішингу, які можуть бути спрямовані на отримання доступу до важливої інформації.

Створення спеціалізованих підрозділів, які будуть зосереджені на захисті персональних даних в умовах воєнного стану, є обов'язковим кроком. Ці команди повинні мати знання та інструменти для реагування на конкретні загрози, пов'язані з конфліктом, а також забезпечувати оперативний моніторинг та реагування на інциденти безпеки, які можуть виникнути в таких умовах (Дяковський, 2022). Вони мають проводити аналіз ризиків та оцінювати ефективність заходів захисту даних, що дозволяє уникнути можливих інцидентів та забезпечити максимальний рівень безпеки для користувачів та організації в цілому. Крім того, спеціалізовані підрозділи можуть забезпечувати навчання персоналу з питань безпеки даних та інформувати їх про нові загрози та заходи захисту. Це допомагає підвищити рівень свідомості користувачів та зменшити ризики виникнення інцидентів.

Створення спеціалізованих підрозділів для захисту персональних даних є ефективним рішенням для компаній та організацій, які мають велику кількість конфіденційної інформації та залежать від безпеки цих даних. Такі підрозділи можуть забезпечити ефективний захист даних та мінімізувати ризики їх втрати, пошкодження або крадіжки. Вони допоможуть підтримувати високий рівень конфіденційності даних, що є критичним для довіри та репутації компанії.

Однак створення спеціалізованих підрозділів може бути витратним і вимагати значних фінансових та інших ресурсів. Наприклад, вони повинні мати належну інфраструктуру, програмне забезпечення та обладнання для виявлення та моніторингу загроз і захисту даних. Також існує ймовірність того, що буде складно знайти кваліфікованих фахівців, які можуть забезпечити високий рівень захисту даних (Капля, 2023).

Отже, створення спеціалізованих підрозділів для захисту персональних даних може бути важливим кроком у забезпеченні безпеки даних та конфіденційності користувачів. Вони дозволять ефективно виявляти й моніторити загрози та проводити аналіз ризиків, що зменшує загрозу втрати даних. Однак при їх створенні необхідно забезпечити достатні ресурси, щоб гарантувати їхню ефективність та адаптивність до нових загроз і викликів.

Розробка та впровадження стратегії кібербезпеки – ще один важливий аспект захисту персональних даних. Організації можуть розробляти та впроваджувати стратегії кібербезпеки, які враховують різноманітні заходи із захисту персональної інформації. Одним із ключових етапів розробки стратегії кібербезпеки є проведення аудиту захисту даних, що дозволяє виявити потенційні слабкі місця та вразливості системи захисту. Наступним етапом є встановлення політики безпеки, яка містить правила та рекомендації щодо захисту даних, враховуючи захист від кібератак, втрати даних і недостовірних даних.

Задля ефективності стратегії кібербезпеки необхідно також забезпечити регулярні оновлення програмного забезпечення та системи захисту даних. Важливо проводити постійний

моніторинг захисних заходів і виявляти потенційні загрози для безпеки даних. Регулярні оновлення та моніторинг захисних заходів дозволяють підтримувати високий рівень безпеки даних та уникати можливих інцидентів.

Окрім цього, розробка стратегії кібербезпеки передбачає також планування екстрених процедур реагування на інциденти, що допомагає швидко відновити роботу системи та мінімізувати наслідки інцидентів. Ефективні екстрені процедури реагування на інциденти можуть значно зменшити ризики втрати даних та негативні наслідки для організації.

Однак розробка та впровадження стратегії кібербезпеки можуть бути витратними і вимагати значних ресурсів. Вона повинна відповідати вимогам законодавства та враховувати особливості конкретної організації. Крім того, для її розробки та впровадження необхідно мати належний рівень експертизи й досвіду, що може викликати певні складнощі.

Таким чином, в умовах воєнного стану в Україні розробка та впровадження стратегії кібербезпеки для захисту персональних даних вимагає особливого підходу. З урахуванням посиленої кіберзагрози й потреби адаптації до незвичайних обставин цей процес повинен зосереджуватися на зменшенні ризиків та запобіганні можливим вторгненням. Однак така розробка може бути витратною, особливо в умовах обмежених ресурсів, що пов'язано з воєнним станом. Тому щоб забезпечити ефективний захист даних, необхідно ретельно планувати стратегії, забезпечити їх регулярне адаптування до умов, що змінюються, та здійснювати безперервний контроль їх ефективності.

Міжнародне співробітництво та обмін досвідом можуть допомогти підвищити рівень захисту персональних даних (Крижна, Кушнір, 2022). У цифрову епоху, коли доступ до інтернету є майже у всіх країнах світу, кібербезпека стає міжнародним питанням, що потребує співпраці різних держав, організацій та компаній.

В умовах воєнного стану в Україні міжнародне співробітництво у сфері кібербезпеки набуває особливого значення. Співпраця може сприяти виявленню нових загроз, що виникають у результаті військових конфліктів, та розробці стратегій для їх нейтралізації. Спільне дослідження та аналіз даних про потенційні кібератаки можуть допомогти ідентифікувати зміни в тактиці злочинців, що пристосовуються до воєнних умов.

Обмін досвідом у цей час може бути незамінним, адже організації, які працюють в умовах конфлікту, стикаються з унікальними викликами та загрозами. Шляхом спільного обговорення можливих рішень та кращих практик можна значно покращити механізми реагування на загрози.

Міжнародні стандарти, такі як GDPR, можуть бути основою, але потребують адаптації до воєнних реалій, зокрема щодо швидкісного реагування на інциденти та підвищення конфіденційності.

Додатково у воєнних умовах особливо актуальним стає міжнародне співробітництво у виявленні та переслідуванні кіберзлочинців. Спільні операції і розслідування можуть не тільки допомогти в попередженні кіберзлочинів, а й демонструвати об'єднану позицію країн проти злочинної діяльності в інтернеті в часи воєнної надзвичайної ситуації. Крім того, міжнародне співробітництво та обмін досвідом можуть допомогти в попередженні кіберзлочинів та виявленні злочинців. Важливою складовою успіху в боротьбі з кіберзлочинністю є співпраця різних країн та організацій у виявленні, переслідуванні та покаранні злочинців. Спільні операції та розслідування можуть допомогти виявити кіберзлочинців та зменшити кількість інцидентів у майбутньому.

Зрештою, міжнародне співробітництво та обмін досвідом є важливими способами підвищення рівня захисту персональних даних. Взаємодія різних держав, організацій та компаній може допомогти виявити нові загрози та розробити спільні стратегії для їх запобігання. Також можна проводити тренінги та навчання фахівців з кібербезпеки, що дозволить підвищити рівень компетентності в цій галузі. Міжнародні стандарти та рекомендації можуть стати базою для розробки внутрішньої політики безпеки даних та захисних заходів. Такі стандарти дозволяють гарантувати високий рівень безпеки даних та підвищують довіру клієнтів і споживачів до організації.

ВИСНОВКИ. Отже, одним із ключових моментів є важливість захисту персональних даних, особливо в таких складних умовах, як воєнний стан. Ефективність застосованих методів реагування на інциденти, їх адаптивність до обставин, що швидко змінюються, та регулярне тестування можуть виявитися першорядними у збереженні конфіденційної інформації. Освіта користувачів щодо можливих загроз та підготовка до них є вирішальним фактором для зменшення ризику злочинних втручань.

Ключові засоби захисту персональних даних в умовах воєнного стану включають у себе фізичний захист об'єктів інформаційної інфраструктури, захист інформаційних систем і

мереж, кібербезпеку та криптографічний захист даних, а також екстрені процедури реагування на інциденти. Для посилення захисту персональних даних важливо проводити освітні заходи, підвищувати обізнаність користувачів, створювати спеціалізовані підрозділи для захисту персональних даних, розробляти та впроваджувати стратегії кібербезпеки, а також здійснювати міжнародне співробітництво й обмін досвідом.

Створення спеціалізованих підрозділів для забезпечення безпеки даних є ефективним, але витратним рішенням, що вимагає відповідної інфраструктури та кваліфікованих фахівців. Ці підрозділи мають можливість реагувати оперативно на загрози, здійснюючи моніторинг і виконуючи розширений аналіз ризиків.

Міжнародне співробітництво слугує додатковим активом у боротьбі з кіберзлочинністю, зокрема в умовах воєнного конфлікту. Співпраця та обмін досвідом між країнами може підвищити рівень захисту даних і прискорити виявлення та реагування на потенційні загрози.

У контексті результатів дослідження запропоновані методи і заходи можуть забезпечити високий рівень безпеки даних та конфіденційності користувачів. Однак їхнє ефективне впровадження вимагає значних ресурсів, спеціалізованого програмного забезпечення та кваліфікованих фахівців. Враховуючи ці методи та результати, можна стверджувати, що розроблені рекомендації дають змогу досягти поставленої мети дослідження, але також наголошують на важливості неперервного моніторингу, адаптації та вдосконалення стратегій захисту даних.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Бем М. В., Городиський І. М. Стандарти захисту персональних даних в соціальній сфері : практ. посіб. Львів, 2018. 110 с.
2. Бем М., Городиський І. Захист персональних даних: правове регулювання та практичні аспекти : наук.-практ. посібник. Київ : К.І.С., 2021. 160 с.
3. Блохін М. Захист персональних даних в умовах війни та воєнного стану // Римське право і сучасність: цивільне право в умовах війни : матеріали Всеукр. наук. конф. (Одеса, 24 трав. 2022 р.) / за заг. ред. Є. О. Харитонова ; Нац. ун-т «Одеська юридична академія». Одеса : Фенікс, 2022. С. 126–129.
4. Джакомопулос К., Буттареллі Д., О'Флаерті М. Посібник з європейського права у сфері захисту персональних даних / пер. В. Кастеллі. Київ : К.І.С., 2018. 436 с.
5. Дяковський О. Захист персональних даних за допомогою правоохоронних органів та суду в умовах війни // Війна та сьогодення. Виклики сучасності : матеріали І Всеукр. наук.-практ. конф. (м. Ірпінь, 2 листоп. 2022 р.) / редкол.: Д. А. Костюк (голова) та ін. Ірпінь, 2022. С. 12–16.
6. Капля О. М. Правове регулювання інформаційної безпеки громадянина під час дії воєнного стану. *Експерт: парадигми юридичних наук і державного управління*. 2023. № 6 (24). С. 16–20. DOI: https://doi.org/10.32689/2617-9660-2022-6(24)-16-20.
7. Кравчук В. О. Захист персональних даних в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2022. № 9. С. 319–321. DOI: https://doi.org/10.32782/2524-0374/2022-9/77.
8. Крижна В., Кушнір І. Щодо обмежень прав людини та правових підстав для обробки персональних даних державними органами в умовах воєнного стану // Регулювання приватно-правових відносин в умовах воєнного стану в Україні : матеріали міжвуз. наук.-практ. конф. (м. Київ, 29 верес. 2022) / МВС України, Нац. акад. внутр. справ. Київ, 2022. С. 191–194.
9. Макушев П. Персональні дані як елемент системи інформаційного забезпечення Державної виконавчої служби України. *Форум права*. 2013. № 2. С. 333–339. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2013_2_51.pdf (дата звернення: 15.08.2023).
10. Павлиш О. Кількість кібератак на Україну продовжує зростати – Держспецзв'язку // Економічна правда : сайт. 10.11.2022. URL: https://www.epravda.com.ua/news/2022/11/10/693694/ (дата звернення: 26.03.2023).
11. Полтораков О. Організаційно-правове забезпечення національної інформаційної безпеки: шляхи вдосконалення // Інтеграція України в Європейське інформаційне суспільство: виклики та завдання / за заг. ред. А. Пазюка. Київ : ФОП Клименко, 2014. С. 225–239.
12. Рогова О. Захист персональних даних у законодавстві Європейського Союзу та України. *Теорія та практика державного управління*. 2011. Вип. 3 (34). С. 464–471.
13. Сопілко І. М. Сучасне поняття персональних даних: доктринальний та нормативний аспекти. *Юридичний вісник*. 2013. № 3 (28). С. 63–68.
14. Худолєй Я. Г., Загребельна Н. А. Захист персональних даних у період дії в Україні правового режиму воєнного стану: загальнотеоретичні аспекти. *Legal Bulletin*. 2023. № 8. С. 75–82. DOI: https://doi.org/10.31732/2708-339X-2023-08-75-82.

15. Semchuk N. Protection of personal data in the law of Ukraine: current status and recommendations for changes // Scientific space: integration of traditional and innovative processes : monograph / H. Dementiiuk, M. Iashchenko, N. Dorogan et al. Riga, Latvia : Baltija Publishing, 2023. Pp. 458–484. DOI: https://doi.org/10.30525/978-9934-26-310-1-18.

Надійшла до редакції: 17.08.2023

Прийнята до опублікування: 20.09.2023

REFERENCES

1. Bem, M. V., & Horoduskyi, I. M. (2018). *Personal data protection standards in the social sphere*. Lviv.

2. Bem, M., & Horoduskyi, I. (2021). *Protection of personal data: legal regulation and practical aspects*. K.I.S.

3. Blokhin, M. (2022, May 24). *Protection of personal data in conditions of war and martial law* [Conference presentation abstract]. All-Ukrainian Scientific Conference "Roman law and modernity: civil law in conditions of war", Odesa, Ukraine.

4. Diakovskyi, O. (2022, November 2). *Protection of personal data with the help of law enforcement agencies and courts in wartime* [Conference presentation abstract]. All-Ukrainian Scientific and Practical Conference "War and the present. Challenges of modernity", Irpin, Ukraine.

5. Giakoumopoulos, C., Buttarelli, D., & O'Flaherty, M. (2018). *Guide to European law in the field of personal data protection* (V. Kastelli, Transl.). K.I.S.

6. Kaplia, O. M. (2023). Legal regulation of citizen's information security during martial law. *Expert: Paradigm of Law and Public Administration, 6*(24), 16–20. https://doi.org/10.32689/2617-9660-2022-6(24)-16-20.

7. Khudoliei, Ya. H., & Zahrebelna, N. A. (2023). Protection of personal data during the period of martial law in Ukraine: general theoretical aspects. *Legal Bulletin, 8*, 75–82. https://doi.org/10.31732/2708-339X-2023-08-75-82.

8. Kravchuk, V. O. (2022). Personal data protection in the conditions of martial law. *Juridical Scientific and Electronic Journal, 9*, 319–321. https://doi.org/10.32782/2524-0374/2022-9/77.

9. Kryzhna, V., & Kushnir, I. (2022, September 29). *Regarding restrictions on human rights and legal grounds for the processing of personal data by state bodies under martial law* [Conference presentation abstract]. Interuniversity Scientific and Practical Conference "Regulation of private legal relations in the conditions of martial law in Ukraine", Kyiv, Ukraine.

10. Makushev, P. (2013). Personal data as an element of the information support system of the State Executive Service of Ukraine. *Forum of Law, 2*, 333–339. http://nbuv.gov.ua/j-pdf/FP_index.htm_2013_2_51.pdf.

11. Pavlysh, O. (2022, November 10). *The number of cyberattacks on Ukraine continues to grow – State Special Communications*. Economic truth. https://www.epravda.com.ua/news/2022/11/10/693694/.

12. Poltorakov, O. (2014). Organizational and legal provision of national information security: ways of improvement. In A. V. Paziuk (Ed.), *Ukraine's integration into the European information society: challenges and tasks*. FOP Klymenko.

13. Rohova, O. (2011). Protection of personal data in the legislation of the European Union and Ukraine. *Theory and Practice of Public Administration, 3*(34), 464–471.

14. Semchuk, N. (2023). Protection of personal data in the law of Ukraine: current status and recommendations for changes. In. H. Dementiiuk, M. Iashchenko, N. Dorogan et al., *Scientific space: integration of traditional and innovative processes.* Baltija Publishing. https://doi.org/10.30525/978-9934-26-310-1-18.

15. Sopilko, I. M. (2013). The modern definition of personal bases: theoretical and legal aspects. *Law Herald, 3*(28), 63–68.

Received the editorial office: 17 August 2023

Accepted for publication: 20 September 2023

VITALII ANATOLIIOVYCH SVITLYCHNYI,
Candidate of Technical Sciences, Associate Professor,
Kharkiv National University of Internal Affairs,
Department of Cybercrime Counteraction;
ORCID: https://orcid.org/0000-0003-3381-3350,
e-mail: vit.svet@ukr.net

PROTECTION OF PERSONAL DATA UNDER MARTIAL LAW IN UKRAINE

The article is devoted to the issue of personal data protection under martial law in Ukraine. A detailed study of this issue has been carried out, aspects of the regulatory environment and levels of personal data protection in such difficult conditions have been considered.

In the context of martial law, the violation of the personal data confidentiality may pose serious threats. It has been highlighted that the disclosure of such data can lead to a risk to the personal safety of people, including those involved in the conflict. This can become the basis for blackmail and manipulation, which negatively affects the situation of individuals and the overall situation.

The recommendations aimed at preventing such threats and improving the level of personal data protection during martial law have been provided. Particular attention has been paid to the need to develop and implement specialised legal acts that would regulate the protection of personal data in such emergency situations. The possibilities of using modern technologies, in particular data encryption and multi-level authentication, to enhance the security and confidentiality of personal data have also been considered.

Implementation of effective personal data protection measures during martial law is an important task to ensure the security and privacy of people. Compliance with regulatory requirements, development of data protection technologies and raising awareness of this issue among the population can help reduce risks and maintain the confidentiality of personal data even in the context of a military conflict.

The conclusions presented in this article can be a valuable source of information for legislators and information security professionals dealing with personal data protection under martial law. The results of the study may contribute to the development and implementation of effective data protection strategies aimed at ensuring the security and privacy of participants to the conflict and citizens in general. Significant aspects of the problem of personal data protection under martial law have been considered and recommendations for improving the situation in this area have been provided.

Key words: *martial law, personal data protection, cybersecurity, legislation, privacy, state security, encryption, access control.*

Цитування (ДСТУ 8302:2015): Світличний В. А. Захист персональних даних в умовах воєнного стану в Україні. *Право і безпека*. 2023. № 3 (90). С. 226–236. DOI: https://doi.org/10.32631/pb.2023.3.19.

Citation (APA): Svitlychnyi, V. A. (2023). Protection of personal data under martial law in Ukraine. *Law and Safety, 3*(90), 226–236. https://doi.org/10.32631/pb.2023.3.19.