УДК 316.77-049.5:355.01]:355.40-049.65
DOI: 10.31866/2617-796X.8.1.2025.335536

Марина Цілина,
кандидат філологічних наук, доцент,
доцент кафедри інформаційної діяльності
та зв'язків з громадськістю,
Київський національний університет
культури і мистецтв,
Київ, Україна
macilin@ukr.net
https://orcid.org/0000-0001-5339-5147

БЕЗПЕКА КОНФІДЕНЦІЙНОЇ ВІЙСЬКОВОЇ ІНФОРМАЦІЇ: ПРОБЛЕМИ, ВИКЛИКИ ТА СПОСОБИ ЗАХИСТУ

Мета статті – виявити основні проблеми й виклики у сфері безпеки конфіденційної військової інформації, з'ясувати способи захисту такої інформації від наявних і потенційних загроз.

Методи дослідження. Застосовано сукупність загальнонаукових методів, зокрема оглядово-аналітичний – для визначення теоретичного підґрунтя наукової розвідки. Системний метод виявився результативним під час вивчення окремих зарубіжних і вітчизняних публікацій, а також розгляду нормативно-законодавчих актів із порушеної проблеми. В основу наукової статті покладено принципи об'єктивності та цілісності.

Наукова новизна полягає в з'ясуванні специфіки роботи з конфіденційною військовою інформацією під час війни в Україні, визначенні переваг і недоліків застосунків «Армія+», «Резерв+», установленні ефективних способів захисту документів та програм редагування інформації обмеженого доступу.

Висновки. Проведене дослідження дало змогу виявити, що найпоширенішими проблемами під час роботи з конфіденційними військовими документами є великий обсяг, контекстуальна чутливість, зміна безпекового середовища, баланс між прозорістю та безпекою, застарілі формати документів, людський чинник, різні стандарти безпеки з країнами-союзниками, можливості супротивника. Вимоги щодо обробки та безпеки персональних даних визначено в спеціальному Порядку Міністерства оборони України. Функціонали застосунків «Армія+», «Резерв+» значно оптимізували діловодні процеси, однак час від часу зазнають кібератак. Окрім самих документів, захищати треба ще й лю-

дей, зокрема військовослужбовців та їхні сім'ї, офіцерів розвідки, звичайних підрядників і цивільних осіб, які співпрацюють з військовими, особовий склад об'єднаних збройних сил, бо вони так само можуть бути мішенями ворога. Стратегії захисту секретної інформації та програмну платформу Redactable, що створені в США, також можна впроваджувати й застосовувати в Україні. Варто завжди пам'ятати, що збої в інформаційній безпеці в армії мають надзвичайно високу ціну, потенційно призводячи до диверсій, загибелі людей і геополітичних наслідків.

Ключові слова: безпека інформації; захист інформації; конфіденційна військова інформація; персональні дані; секретні документи.

Вступ. Війна Росії проти України, окрім деструктивних і часто непоправних змін у житті людей, принесла цілу низку викликів і проблем, які стали необхідними й нагальними для вирішення. Серед таких варто виокремити аспект безпеки конфіденційної військової інформації, оскільки це питання також тісно пов'язане не тільки із захистом окремих військових структур, а й із функціонуванням держави в цілому.

Великі обсяги секретних військових документів, система безпеки, яка швидко розвивається, і постійні зовнішні та внутрішні загрози є одними з найбільших проблем у сфері конфіденційної військової інформації. З огляду на катастрофічні наслідки витоку військових даних важливо подолати ці труднощі та забезпечити військову інформаційну безпеку.

Результати дослідження. Порушену тему поодиноко зачіпали в деяких вітчизняних публікаціях, але через обмеженість доступу до інформації із зрозумілих причин її не вдавалося вповні розкрити. Тому загальні аспекти можна дізнатися або від уповноважених державних органів, або від юристів і журналістів. Д. Воюта (2022) пропонує низку інформаційних роз'яснень щодо того, як захистити персональні дані військовослужбовців; Х. Ярмакі та С. Музика (2022) розглянули питання конфіденційної інформації в органах Національної поліції України під час режиму воєнного стану; І. Лаб'як (2024) дає інформацію про застосунок «Резерв+»; П. Адамс (2023) із BBC News Україна – про злив секретних документів США про Україну. Проведенню дослідження спряли вебсторінки Міністерства оборони України, Укрінформ, команди реагування на комп'ютерні надзвичайні події України CERT UA та американської компанії Redactable.

Робота з конфіденційними військовими документами може охоплювати такі найпоширеніші проблеми:

1. Значні обсяги документів: під час воєнних дій регулярно створюється велика кількість документів, зокрема секретні розвідувальні звіти, оперативні плани, документи матеріально-технічного забезпечення та звіти про завершення дій. Щоб запобігти витокам, необхідно здійснити редагування всіх цих документів за нормами й правилами. Проте інколи застарілі методи редагування вручну є повільними, громіздкими та схильними до помилок. Такі підходи піддають ризику конфіденційну інформацію та національну безпеку.

2. Контекстуальна чутливість: у військових документах інформація, яка з першого погляду ніби здається нешкідливою, може бути засекречена через її зв'язок з іншими даними в тому самому документі, навіть одне порушення даних може

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

призвести до непоправного. Ураховуючи цю контекстуальну чутливість, можна уникнути значних помилок.

3. Зміна безпекового середовища: оскільки державні установи та військові відомства продовжують використовувати цифрові взаємозв'язки, нові платформи можуть створювати непередбачені прогалини в захисті. Документи можуть надаватися через пристрої IoT або вводитися в інструменти ШІ без належного редагування, тому потенційно конфіденційна інформація може залишитися відкритою. Щоб протистояти новим загрозам, треба постійно адаптувати практику редагування.

4. Між прозорістю та безпекою. Департаменти повинні виконувати запити на публічну інформацію, водночас захищаючи інтереси національної безпеки. Державні службовці часто стикаються з тиском, щоб бути прозорими, а це значно збільшує ризик поспішного редагування для задоволення вимог засобів масової інформації. Це посилює потребу у вдосконаленій, швидшій і простішій у використанні системі редагування документів.

5. Застарілі формати документів: багатьом співробітникам військових відомств також доводиться керувати різними типами документів, охоплюючи історичні паперові записи та застарілі цифрові формати. Це створює унікальні проблеми для редагування вручну, такі як непослідовне форматування, відсутність чітких метаданих і фізична крихкість.

6. Людський чинник є ще однією ключовою загрозою безпеці військових документів. Це можуть бути не тільки зовнішні, а й внутрішні загрози (наприклад, агенти іноземної розвідки чи незадоволені співробітники), людські помилки та вразливі місця соціальної інженерії. Ці недоліки часто важко виявити, але вони призводять до серйозних порушень безпеки.

7. Під час проведення спільних операцій із союзниками конфіденційну інформацію повинні передавати між кількома мережами з країнами, які мають різні стандарти безпеки. Без належного редагування це створює прогалини, які можуть стати причиною шпигунства чи витоку інформації.

8. Можливості супротивника: спонсоровані ворогом шпигунські групи мають значні фінансові й технічні ресурси, які вони можуть використовувати для атак на мережі та порушення безпеки документів. Тому важливо забезпечити повну й надійну редакцію військових документів перед розповсюдженням.

9. Вразливості ланцюга постачання: конфіденційна військова інформація також може бути розкритою через компрометацію апаратного чи програмного забезпечення від постачальників. Однак редагуючи документи перед тим, як зберігати їх у наданих постачальниками системах, військові відомства можуть значно зменшити цей ризик.

З лютого 2022 року значно збільшилася кількість військовослужбовців, тому захист їхніх персональних даних набув додаткової актуальності. Вимоги щодо обробки та безпеки персональних даних визначено в спеціальному Порядку Міністерства оборони України. Передбачено бази персональних даних, де є військовослужбовці, працівники, державні службовці, військовозобов'язані, призовники, резервісти, особи, звільнені з військової служби, ветерани військової служби та війни.

У таких базах обробляються: прізвище, ім'я, по батькові; дата і місце народження; паспортні дані, ІПН; відомості про освіту, стан здоров'я, про сімейний

стан, фактичне місце проживання; номери телефонів; відомості, що підтверджують право на пільги та компенсації; відомості про проходження військової (державної) служби; відомості про військовий облік; відомості про трудову діяльність, що містяться в трудовій книжці, а також інші персональні дані, що дають можливість ідентифікувати особу та необхідність обробки яких визначена чинним законодавством (Верховна Рада України, 2014).

Обробку та захист персональних даних у формі картотеки здійснюють з урахуванням таких вимог:

– документи з персональними даними формуються у справи (картки) з метою обробки персональних даних;

– справи з документами, які містять персональні дані, повинні мати внутрішні описи документів;

– справи (картки) мають зберігатися у спеціальних приміщеннях (сейфах, металевих шафах), що надійно замикаються й опечатуються;

– приміщення обладнані охоронною й пожежною сигналізаціями;

– двері приміщень (сейфів, металевих шаф) мають бути з надійними замками з двома екземплярами ключів.

Якщо ідеться про персональні дані, що обробляються в інформаційно-телекомунікаційних системах, то цей процес здійснюється із забезпеченням захисту персональних даних за нормативно-правовими актами в галузі безпеки інформації. Обробляючи персональні дані в інформаційно-телекомунікаційній системі, треба застосовувати комплексну систему захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, установленому чинним законодавством.

Необхідно встановити захист реєстраційних даних від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, поширення. Тому в інформаційно-телекомунікаційній системі треба обов'язково реєструвати:

– результати ідентифікації та автентифікації користувачів;

– результати виконання користувачем операцій з обробки інформації;

– спроби несанкціонованих дій з інформацією;

– факти надання та позбавлення користувачів права доступу до інформації та її обробки;

– результати перевірки цілісності засобів захисту інформації.

Служба захисту інформації повинна створити та забезпечити функціонування комплексних систем захисту інформації в інформаційно-телекомунікаційній системі.

Командири або начальники структурних підрозділів вживають необхідних організаційних і технічних заходів для того, щоб забезпечити процедуру обробки персональних даних згідно з чинним законодавством, зокрема:

– організовують належну охорону території військової частини та перепускний режим;

– установлюють режим доступу до компонентів фізичного середовища інформаційно-телекомунікаційної системи;

– контролюють надійне зберігання магнітних, оптичних, паперових та інших носіїв інформації;

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

– залучають до використання засоби захисту інформації, що мають позитивний експертний висновок або сертифікат відповідності.

Усі процеси, пов'язані зі збиранням, реєстрацією, накопиченням, зберіганням, адаптуванням, зміною, поновленням, використанням і поширенням (розповсюдженням, реалізацією, передачею), знеособленням, знищенням та захистом персональних даних, покладено на особу (осіб), яку (яких) визначив командир (начальник).

У травні 2024 року Міністерство оборони України розробило український мобільний застосунок «Резерв+», який дає змогу призовникам, військовозобов'язаним та резервістам оновити свої облікові дані й отримати електронний військово-обліковий документ. Із 18 червня в цьому застосунку став доступний електронний військово-обліковий документ, що має таку ж юридичну силу, як і паперовий. За допомогою нового функціоналу ТЦК та поліція можуть перевірити чинність документа, скануючи QR-код через камеру на смартфоні. Для того щоб у «Резерв+» підтягнуло військовий квиток, необхідно оновити застосунок та натиснути кнопку «згенерувати документ».

У застосунку «Резерв+» є доступ до таких даних (Міністерство оборони України, 2024), як:

– прізвище, ім'я, по батькові особи;
– вид обліку / дата зняття (виключений);
– категорії обліку;
– дата народження;
– відстрочки / бронювання / дата закінчення;
– постанова ВЛК / дата ВЛК;
– звання;
– код і найменування військово-облікової спеціальності;
– податковий номер (РНОКПП);
– унікальний номер у реєстрі «Оберіг»;
– ТЦК та СП, де особа перебуває на обліку;
– чи подано особу в розшук.

Специфіка застосунку «Резерв+» полягає в тому, що на серверній частині взагалі не зберігаються персональні дані користувачів. Інформація передається тільки зашифровано. Серверна частина системи розгорнута в хмарній інфраструктурі, що має необхідні сертифікати безпеки, зокрема атестат відповідності комплексній системі захисту інформації (КСЗІ).

Варто зазначити, що урядова команда реагування CERT-UA в жовтні 2024 року отримала інформацію щодо розповсюдження через обліковий запис @reserveplusbot повідомлень про необхідність установлення «спеціального програмного забезпечення» із прикріпленим архівом «RESERVPLUS.zip». Установлено, що архів містить шкідливе програмне забезпечення MEDUZASTEALER, яке здійснює викрадення файлів. Обліковий запис @reserveplusbot створено під виглядом телеграмбота, що імітує технічну підтримку застосунку для призовників, військовозобов'язаних і резервістів «Резерв+». Необхідно звернути увагу на те, що такий обліковий запис у травні 2024 року дійсно зазначався як один з контактів технічної підтримки «Резерв+». З'ясувавши деталі інциденту, команда CERT-UA мінімізувала такі загрози (Зафіксовано поширення шкідливих програм, 2024).

У серпні 2024 року запущено інший цифровий застосунок «Армія +». Директор Директорату цифрової трансформації у сфері оборони Міністерства оборони України Артем Романюков зазначив, що той масив інформації, яку можна отримати ворогу, захопивши, наприклад, паперовий військово-обліковий документ, військовий квиток, і те, що є в застосунку, є неспівмірним, бо в паперовому її більше (У Міноборони розповіли про захист інформації, 2024). Застосунок має дві основні функції: перша – це військовий ID; друга – електронні рапорти, яких 11 (до переліку ввійшли найпоширеніші). Електронні рапорти мають ту саму юридичну силу, що й паперові. Однак водночас є і низка викликів. По-перше, з авторизацією, бо застосунок працює через Реєстр призовників, військовозобов'язаних та резервістів, відомий як «Оберіг», і цілком зрозумілим стало очікування, що буде певний відсоток людей, які не зможуть авторизуватися, бо система їх не змогла ідентифікувати як військовослужбовців. Тому окремо створено невеличку команду, що опрацьовує такі кейси для того, щоб у Реєстрі швидко, проте з підтвердженням і цілком законно усунути ту незручність, коли людина не змогла себе знайти.

Іншим викликом А. Романюков назвав користування вже самою системою. Функція Армія ID – це 9-значний унікальний код, який отримує кожен військово службовець у системі. І з міркувань безпеки, щоб не подавати рапорт на конкретну посаду з конкретним прізвищем, він подається на Армії ID кожного командира. Нині військовослужбовці можуть дізнатися Армії ID своїх командирів, щоб мати можливість звертатися з рапортами. Однак для початку необхідно встановити застосунок «Армія+» на пристрої командирів.

Якщо говорити про наявний функціонал, то директор Директорату цифрової трансформації зауважив, що можна зекономити десятки годин роботи людей, військовослужбовців Збройних сил, оптимізувавши ці діловодні процеси: «Навіть за найбільш скромними підрахунками, на рік ми вивільнимо близько 60 робочих годин для кожного підрозділу на рівні батальйону» (У Міноборони розповіли про захист інформації, 2024).

17.12.2024 урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA від фахівців MIL.CERT-UA отримала інформацію щодо виявлення низки вебресурсів, які імітують офіційну сторінку застосунку «Армія+» та опубліковані за допомогою сервісу Cloudlfare Workers (Кібератака UAC-0125, 2024).

Користувачам, які відвідували згадані вебсайти, пропонували завантажити файл «ArmyPlusInstaller-v.0.10.23722.exe» (назва змінювалася).

Установлено, що EXE-файл є інсталятором, який створений за допомогою NSIS (Nullsoft Scriptable Install System), що, окрім .NET файлу-приманки «ArmyPlus.exe», містить файли інтерпретатора Python, архів із файлами програми Tor, а також PowerShell-скрипт «init.ps1».

Коли відкрити файл «ArmyPlusInstaller-v.0.10.23722.exe», то запуститься файл-приманка, а також PowerShell-скрипт з метою:

– здійснити інсталяцію сервера OpenSSH на електронно-обчислювальну машину цільової системи;
– згенерувати пару RSA-ключів;
– додати публічний ключ до файлу «authorized_keys» для автентифікації;

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

– відправити приватний ключ за допомогою «curl» на сервер зловмисників (TOR-адреса);

– опублікувати прихований SSH-сервіс за допомогою Tor.

У такий спосіб створиться технічна можливість для віддаленого прихованого доступу до електронно-обчислювальної машини цільової системи, що становить потенційну загрозу інформаційній безпеці. До того ж успішно проникнувши та зацікавившись об'єктом впливу, зловмисники надалі розвивають кібератаку на інформаційно-комунікаційну систему організації.

У 2022 році в США стався великий військовий витік, коли Джек Тейшейра нібито опублікував секретні військові документи в чаті онлайн-ігор. Цей витік виявив велику складність покращення безпеки документів в уряді без упровадження політики, яка перешкоджає можливості обмінюватися важливою інформацією з урядом, коли це необхідно.

Найбільшим був витік секретної інформації, яку мали США, про війну (за більш ніж рік після повномасштабного вторгнення Росії до України). Як зазначали анонімні чиновники з Пентагону, це понад 100 документів з датами, численними військовими абревіатурами, деякі під грифом «цілком таємно», з детальною картиною війни в Україні. У них ішлося про втрати обох боків, про їхні слабкі сторони і, що важливо, про співвідношення сил у можливому весняному наступі України у 2023 році (Адамс, 2023).

Військові операції створюють значні обсяги записів і документів, що треба зредагувати, щоб зв'язок залишався плавним, а секретність зберігалася за принципом «необхідно знати».

Є особи, які мають бути захищені під час роботи з військовими документами. Деякі групи стають особливо вразливими, коли конфіденційна військова інформація не захищена належним чином, зокрема (How to protect military classified documents?, 2025):

1. Військовослужбовці: члени служби та їхні сім'ї стикаються з ризиком викрадення особистих даних, переслідувань або цілеспрямованих атак у разі розголошення їхньої особистої інформації.

2. Офіцери розвідки, які беруть участь у зборі розвіданих, також можуть опинитися під загрозою з боку ворогів, які прагнуть підірвати їхні операції чи помститися їм особисто.

3. Звичайні підрядники й цивільні особи, які співпрацюють з військовими, часто можуть мати доступ до конфіденційної інформації і стати мішенню, якщо їхні дані не будуть захищеними.

4. Особовий склад об'єднаних збройних сил. Члени держав-союзників теж опиняються під загрозою в разі витоку спільної конфіденційної інформації, а це потенційно може погіршити міжнародні відносини.

Збройні сили США використовують різні стратегії для захисту секретної інформації, де поєднуються традиційні практики з передовими технологіями. Ці стратегії охоплюють (How to protect military classified documents?, 2025):

1. Редагування документів військової таємниці

Редагування, як правило, використовується для того, щоб видалити чи приховати конфіденційні деталі з документів перед ширшим розповсюдженням або розсекреченням. Це дає можливість організаціям зберігати публічні записи, одночасно захищаючи конфіденційні дані.

2. Заходи фізичної безпеки

Військові обробляють багато фізичних документів, тому створили зони обмеженого доступу, відомі як Sensitive Compartmented Information Facilities (SCIF), для зберігання та захисту конфіденційних документів. Вони також передбачили контрольовані методи утилізації секретних матеріалів, включаючи спалювання, подрібнення та виготовлення целюлози.

3. Цифрове шифрування

Розширені протоколи шифрування гарантують безпечний електронний зв'язок і зберігання даних. Уряд США вимагає використання шифрування AES-128 для несекретної інформації та шифрування AES-256 для надсекретної інформації.

4. Допуск персоналу

Для усунення людського чинника військові відомства проводять ретельну перевірку даних і призначають рівні доступу особам, які мають доступ до конфіденційної інформації. Чотири основні типи допуску безпеки: конфіденційна, секретна, цілком таємна та конфіденційна інформація (SIC).

5. Захищені канали зв'язку

Для запобігання несанкціонованому перехопленню конфіденційних комунікацій військові використовують спеціальні зашифровані мережі для передачі секретних даних. Ці безпечні канали захищені від прослуховування та кібервійни, забезпечуючи захист даних під час передачі між підрозділами та базами.

6. Системи класифікації інформації

Військові організовують конфіденційну інформацію в ієрархію відповідно до її конфіденційності та потенційного впливу її компрометації. Більш високий рівень конфіденційності отримує додатковий захист для запобігання розголошенню інформації.

7. Протоколи кібербезпеки

Для цифрової інформації відділи використовують передові брандмауери та системи виявлення вторгнень, а також проводять регулярні перевірки безпеки цифрової інфраструктури. Виявлені оцінки вразливості дають змогу усунути потенційні недоліки в системі, забезпечуючи захист військової інфраструктури як від хакерів, так і від кібервійни з боку суб'єктів державного рівня.

8. Програми навчання та підвищення обізнаності

Військовослужбовці проходять регулярні тренінги з найкращих практик інформаційної безпеки та потенційних загроз, що охоплюють низку передових методів захисту конфіденційної інформації. Ідеться про виявлення спроб фішингу та розпізнавання спроб соціальної інженерії.

Збої в інформаційній безпеці в армії мають надзвичайно високу ціну, адже потенційно призводять до геополітичних наслідків, диверсій і загибелі людей. Тому державні службовці повинні забезпечити постійний захист конфіденційних документів. Проте неможливим є ефективне та послідовне впровадження реда-

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

гування вручну через великі обсяги документів і підвищену контекстну чутливість. Є сучасне рішення для редагування – Redactable.

Платформа Redactable, розроблена згідно із суворими вимогами безпеки військових і оборонних організацій, на основі штучного інтелекту автоматизує процес редагування. Функції Redactable, що дають змогу забезпечити максимальний захист військової інформації (How to protect military classified documents?, 2025):

1. Протоколи безпеки військового рівня: найвищий рівень шифрування та заходи безпеки для захисту секретної інформації у процесі редагування. Контекстне редагування на основі штучного інтелекту: удосконалені алгоритми ідентифікують і редагують конфіденційну інформацію на основі контексту, а не тільки ключових слів.

2. Правила класифікації, що можна налаштувати: Redactable дає змогу створювати правила редагування, що узгоджуються з конкретними системами військової класифікації та протоколами безпеки.

3. Ефективно обробляє великі обсяги секретних документів, що значно спрощує процес редагування великих військових записів.

4. Підтримує багато форматів: обробляє різні типи документів, що часто використовуються у військових умовах, зокрема скановані історичні записи та цифрові файли.

5. Аудиторські журнали та звітність про відповідність: забезпечує повну реєстрацію всіх дій редагування, підтримуючи військові вимоги відповідності та звітності.

6. Функції безпечної співпраці: дає можливість уповноваженому персоналу керувати обміном і переглядом зредагованих документів, підтримуючи безпеку роботи.

Висновки. Найпоширенішими проблемами під час роботи з конфіденційними військовими документами є великий обсяг, контекстуальна чутливість, зміна безпекового середовища, баланс між прозорістю та безпекою, застарілі формати документів, людський чинник, різні стандарти безпеки з країнами-союзниками, можливості супротивника. Вимоги щодо обробки і безпеки персональних даних визначено в спеціальному Порядку Міністерства оборони України. Функціонали застосунків «Армія+», «Резерв+» значно оптимізували діловодні процеси, однак час від часу зазнають кібератак. Окрім самих документів, захищати треба ще й людей, зокрема військовослужбовців та їхні сім'ї, офіцерів розвідки, звичайних підрядників і цивільних осіб, які співпрацюють з військовими, особовий склад об'єднаних збройних сил, бо вони так само можуть бути мішенями ворога. Стратегії захисту секретної інформації та програмну платформу Redactable, що створені в США, також можна впроваджувати й застосовувати в Україні.

СПИСОК ПОСИЛАНЬ

Адамс, П., 2023. Злив секретних документів США по Україні: про що він нам розповів. *BBC News Україна*, [online] 10 квітня. Доступно: <https://www.bbc.com/ukrainian/features-65229785> [Дата звернення 29 березня 2025].

Верховна Рада України, 2014. *Про затвердження Порядку обробки і захисту персональних даних у Міністерстві оборони України, Наказ Міністерства оборони України №926 від 26.12.2014*. [online] Доступно: <https://zakon.rada.gov.ua/laws/show/z0071-15#Text> [Дата звернення 29 березня 2025].

Воюта, Д., 2022. Як захистити персональні дані: права військовослужбовців. *Центр демократії та верховенства права*, [online] 22 грудня. Доступно: <https://cedem.org.ua/consultations/yak-zahystyty-personalni-dani-prava-vijskovosluzhbovtsiv/> [Дата звернення 29 березня 2025].

Зафіксовано поширення шкідливих програм через Telegram нібито від технічної підтримки «Резерв+», 2024. *Державна служба спеціального зв'язку та захисту інформації України,* [online] 16 жовтня. Доступно: <https://cip.gov.ua/ua/news/zafiksovano-poshirennya-shkidlivikh-program-cherez-telegram-nibito-vid-tekhnichnoyi-pidtrimki-rezerv> [Дата звернення 29 березня 2025].

Кібератака UAC-0125 з використанням тематики «Армія+» (CERT-UA#12559), 2024. *CERT-UA*. [online] Доступно: <https://cert.gov.ua/article/6281701> [Дата звернення 29 березня 2025].

Лаб'як, І., 2024. Усе про застосунок «Резерв+»: для чого він потрібен, які документи містить і навіщо там QR-код. *ТСН*, [online] 18 червня. Доступно: <https://tsn.ua/exclusive/use-pro-rezerv-2602749.html> [Дата звернення 29 березня 2025].

Міністерство оборони України, 2024. *Резерв+: сторінка застосунку призовників, військовозобов'язаних та резервістів*. [online] Доступно: <https://reserveplus.mod.gov.ua/> [Дата звернення 29 березня 2025].

У Міноборони розповіли про захист інформації в застосунку «Армія+», 2024. *Укрінформ*, [online] 13 серпня. Доступно: <https://www.ukrinform.ua/rubric-society/3894795-u-minoboroni-rozpovili-pro-zahist-informacii-v-zastosunku-armia.html> [Дата звернення 29 березня 2025].

Ярмакі, Х.П. та Музика, С.С., 2022. Щодо питання конфіденційної інформації в органах національної поліції України під час режиму воєнного стану. *Південноукраїнський правничий часопис*, [e-journal] 1-2, с.194-199. https://doi.org/10.32850/sulj.2022.1-2.34

How to protect military classified documents?, 2025. *Redactable*, [online] 25 March. Available at: <https://www.redactable.com/blog/how-to-protect-sensitive-military-information> [Accessed 29 March 2025].

REFERENCES

Adams, P., 2023. Zlyv sekretnykh dokumentiv SShA po Ukraini: pro shcho vin nam rozpoviv [The leak of classified US documents on Ukraine: what he told us]. *BBC News Ukraina*, [online] 10 April. Available at: <https://www.bbc.com/ukrainian/features-65229785> [Accessed 29 March 2025].

How to protect military classified documents?, 2025. *Redactable*, [online] 25 March. Available at: <https://www.redactable.com/blog/how-to-protect-sensitive-military-information> [Accessed 29 March 2025].

Kiberataka UAC-0125 z vykorystanniam tematyky "Armiia+" (CERT-UA#12559) [UAC-0125 Cyberattack Using the "Army+" Theme (CERT-UA#12559)], 2024. *CERT-UA*. [online] Available at: <https://cert.gov.ua/article/6281701> [Accessed 29 March 2025].

Labiak, I., 2024. Use pro zastosunok "Rezerv+": dlia choho vin potriben, yaki dokumenty mistyt i navishcho tam QR-kod [All about the "Reserve+" application: what it is for, what documents

ISSN 2617-796X (print)
ISSN 2618-0049 (online)

it contains and why there is a QR code]. *TSN*, [online] 18 June. Available at: <https://tsn.ua/exclusive/use-pro-rezerv-2602749.html> [Accessed 29 March 2025].
Ministry of Defence of Ukraine, 2024. *Rezerv+: storinka zastosunku pryzovnykiv, viiskovozoboviazanykh ta rezervistiv* [Reserve+: application page for conscripts, military personnel and reservists]. [online] Available at: <https://reserveplus.mod.gov.ua/> [Accessed 29 March 2025].
U Minoborony rozpovily pro zakhyst informatsii v zastosunku "Armiia+" [The Ministry of Defense spoke about the protection of information in the "Army+" application], 2024. *Ukrinform*, [online] 13 August. Available at: <https://www.ukrinform.ua/rubric-society/3894795-u-minoboroni-rozpovili-pro-zahist-informacii-v-zastosunku-armia.html> [Accessed 29 March 2025].
Verkhovna Rada of Ukraine, 2014. *Pro zatverdzhennia Poriadku obrobky i zakhystu personalnykh danykh u Ministerstvi oborony Ukrainy* [On approval of the Procedure for processing and protecting personal data in the Ministry of Defense of Ukraine], Order of the Ministry of Defense of Ukraine No. 926 of 26.12. 2014. [online] Available at: <https://zakon.rada.gov.ua/laws/show/z0071-15#Text> [Accessed 29 March 2025].
Voiuta, D., 2022. Yak zakhystyty personalni dani: prava viiskovosluzhbovtsiv [How to protect personal data: the rights of military personnel]. *Centre for Democracy and Rule of Law*, [online] 22 December. Available at: <https://cedem.org.ua/consultations/yak-zahystyty-personalni-dani-prava-vijskovosluzhbovtsiv/> [Accessed 29 March 2025].
Yarmaki, Kh.P. and Muzyka, S.S., 2022. Shchodo pytannia konfidentsiinoi informatsii v orhanakh natsionalnoi politsii Ukrainy pid chas rezhymu voiennoho stanu [Regarding the issue of confidential information in the bodies of the National Police of Ukraine during the martial law regime]. *South Ukrainian Law Journal*, [e-journal] 1-2, pp.194-199. https://doi.org/10.32850/sulj.2022.1-2.34
Zafiksovano poshyrennia shkidlyvykh prohram cherez Telegram nibyto vid tekhnichnoi pidtrymky "Rezerv+" [Malware spread via Telegram allegedly from technical support of "Rezerv+" was recorded], 2024. *State Service of Special Communications and Information Protection of Ukraine*, [online] 16 October. Available at: <https://cip.gov.ua/ua/news/zafiksovano-poshirennya-shkidlivikh-program-cherez-telegram-nibito-vid-tekhnichnoyi-pidtrimki-rezerv> [Accessed 29 March 2025].

UDK 316.77-049.5:355.01]:355.40-049.65

Maryna Tsilyna,
PhD in Philology, Associate Professor,
Associate Professor at the Department
of Information Activities and Public Relations,
Kyiv National University of Culture and Arts,
Kyiv, Ukraine
macilin@ukr.net
https://orcid.org/0000-0001-5339-5147

SECURITY OF CONFIDENTIAL MILITARY INFORMATION: PROBLEMS, CHALLENGES AND METHODS OF PROTECTION

The purpose of the research in the article is to identify the main problems and challenges in the security of confidential military information, and to find ways to protect such information from existing and potential threats.

The research methodology is outlined as are general scientific methods, in particular survey and analytical methods, that are used to determine the theoretical basis of scientific research. The systematic method proved effective during the study of individual foreign and domestic publications and the consideration of regulatory and legislative acts on the problem raised. The scientific article is based on the principles of objectivity and integrity.

The scientific novelty consists in clarifying the specifics of working with confidential military information during the war in Ukraine, determining the advantages and disadvantages of the «Army+» and «Reserve+» applications, and establishing effective methods of protecting documents and programs for editing restricted access information.

Conclusions. The conducted research made it possible to reveal that the most common problems when working with confidential military documents are a large volume, contextual sensitivity, the development of the security landscape, the balance between transparency and security, outdated document formats, the human factor, different security standards with allied countries, and the capabilities of the adversary. The requirements for the processing and security of personal data are defined in the special Procedure of the Ministry of Defence of Ukraine. Functionalities of the «Army+» and «Reserve+» applications have significantly optimised business processes, but they are subject to cyberattacks occasionally. In addition to the documents themselves, it is also necessary to protect people, including military personnel and their families, intelligence officers, ordinary contractors and civilians who cooperate with the military, personnel of the combined armed forces, because they can also be enemy targets. Secret information protection strategies and the Redactable software platform, created in the USA, can also be applied and implemented in Ukraine. It should always be remembered that information security failures in the military come at an extremely high cost, potentially leading to sabotage, loss of life and geopolitical consequences.

Keywords: information security; information protection; confidential military information; personal data; secret documents.

Надійшла 31.03.2025
Прийнята 22.05.2025
Стаття була вперше опублікована онлайн 18.07.2025

ISSN 2617-796X (print)
ISSN 2618-0049 (online)