DOI: 10.33270/05267303.16
УДК 004.056:351.74(477)

КУДІНОВ Вадим*
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
ORCID: https://orcid.org/0000-0002-5299-0590;
ТАРАСЕНКО Володимир
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
ORCID: https://orcid.org/0009-0005-0250-7678;
ШВЕЦЬ Микола
викладач кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
ORCID: https://orcid.org/0000-0002-8489-4659

Напрями вдосконалення кіберзахисту інформаційних систем спеціального призначення МВС України в умовах воєнного стану

Анотація. В умовах воєнного стану й гібридної агресії з боку російської федерації інформаційні системи України щодня зазнають близько 15 цілеспрямованих кібератак. У цей період украй вразливими є об'єкти критичної інфраструктури держави, серед яких вагоме місце посідають інформаційні системи спеціального призначення Міністерства внутрішніх справ України. Зазначені відомчі ресурси забезпечують безперервний інформаційно-аналітичний супровід повсякденної діяльності правоохоронних органів, підрозділів Національної поліції України й екстрених служб швидкого реагування. Попри значну кількість наукових праць у галузі захисту інформації, комплексний підхід до системної нейтралізації різних типів сучасних кібератак на такі специфічні системи досі залишається недостатньо дослідженим в українському науковому дискурсі. Наявні методичні підходи переважно фокусуються на протидії окремим видам загроз без урахування системних взаємозв'язків усередині єдиної інформаційної системи відомства. Метою статті є обґрунтування перспективних напрямів удосконалення кіберзахисту та підвищення загального рівня кіберстійкості інформаційних систем спеціального призначення Міністерства внутрішніх справ України в сучасних умовах. У межах дослідження детально проаналізовано ключові загрози, зумовлені ймовірними типами кібератак на відомчі інформаційні системи, а також визначено найкритичніші вразливості чинних контурів безпеки. На основі отриманих аналітичних даних запропоновано комплексний підхід до підвищення їхньої кіберстійкості. Сформульовано практичні рекомендації щодо мінімізації негативного впливу кіберінцидентів на загальний рівень захищеності інформаційних систем спеціального призначення Міністерства внутрішніх справ України, що сприятиме підвищенню стійкості функціонування підрозділів до кіберзагроз.

Ключові слова: кібербезпека; кіберстійкість; об'єкти критичної інфраструктури; інформаційні системи спеціального призначення; МВС України; Національна поліція України; кібератака; захист інформації.

Історія статті:
Отримано: 30.06.2026
Прийнято: 01.09.2026
Опубліковано: 01.10.2026

Рекомендоване посилання:
Кудінов В., Тарасенко В., Швець М. Напрями вдосконалення кіберзахисту інформаційних систем спеціального призначення МВС України в умовах воєнного стану. *Наука і правоохорона.* 2026. Вип. 3 (73). С. 177–186. DOI: 10.33270/05267303.16

*Відповідальний автор

© Кудінов В., Тарасенко В., Швець М., 2026. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

Вступ

Стрімка цифровізація всіх сфер суспільного життя в Україні, зокрема правоохоронної діяльності, супроводжується масштабним зростанням кіберзагроз. Особливо небезпечними є цілеспрямовані кібератаки на інформаційні системи спеціального призначення (далі – ІССП) Міністерства внутрішніх справ (далі – МВС) України. Це зумовлено тим, що правопорушники активно застосовують новітні інформаційні технології, зокрема системи штучного інтелекту (далі – ШІ), для модернізації методів компрометації даних.

У МВС України протягом останнього десятиліття вживають заходів щодо створення нових та удосконалення вже наявних ІССП у складі єдиної інформаційної системи (далі – ЄІС) МВС України. Зокрема, у Положенні про єдину інформаційну систему МВС зазначено: «ЄІС МВС – інтегрована інформаційна система, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їхньої діяльності й становить сукупність взаємозв'язаних функціональних підсистем, сервісів, програмно-інформаційних комплексів, програмно-технічних і технічних засобів електронної комунікації»[1].

Однією із важливих ІССП ЄІС МВС є інформаційно-комунікаційна система «Інформаційний портал Національної поліції України»[2] (далі – ІПНП). Її головне завдання полягає в інформаційно-аналітичному забезпеченні діяльності Національної поліції України (далі – НПУ). Інформацію з цієї системи використовують: 1) для наповнення та підтримки в актуальному стані баз (банків) даних, які входять до ЄІС МВС та визначені ст. 26 Закону України «Про Національну поліцію»[3]; 2) для формування баз даних у сфері управлінських відносин, необхідних для виконання покладених на поліцію повноважень; 3) для формування баз даних, необхідних для забезпечення щоденної діяльності поліції, у сфері трудових відносин, фінансового забезпечення, документообігу.

Важливість інформації, яка обробляється в ІССП МВС України, зокрема НПУ, полягає в її належності до державних інформаційних ресурсів. Відповідно, вона не підлягає поширенню та передачі іншим особам, крім випадків, передбачених законодавством.

В Україні останнім часом фіксують близько 15 кібератак щодня, переважно з боку рф, спрямованих на державний сектор і критичну інфраструктуру. Зокрема, у першій половині 2025 року Україна посіла п'яте місце у світі й третє в Європі за кількістю кібератак проти країни. Такі дані наводить Digital Defense Report 2025, оприлюднені компанією Microsoft. У глобальному розподілі загроз перші місця посідають США (24,8%), Велика Британія (5,6 %), Ізраїль (3,5 %), Німеччина (3,3 %), а Україна має 2,8 % від загального обсягу атак[4].

За даними Держспецзв'язку та команди CERT-UA, станом на 2025–2026 роки Україна залишається однією з головних цілей кібератак у світі. Кількість інцидентів щороку зростає: лише за 2025 рік було опрацьовано майже 6000 кібератак, що на 37 % більше, ніж у попередньому році. За даними CERT-UA, найактивнішими є російські угруповання, такі як Gamaredon (UAC-0010), також відомий як Armagedon[5].

Для протидії кіберзагрозам державному сектору та критичній інфраструктурі на державному рівні прийнято Указ Президента України № 447/2021 «Про Стратегію кібербезпеки України», який є документом стратегічного планування високого рівня[6]. Кіберстійкість країни в цьому Указі визначено через такі стратегічні завдання: 1) посилення кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури; 2) підвищення рівня цифрової грамотності, кіберобізнаності щодо сучасних кіберзагроз і протидії їм населенням України.

У сучасних умовах воєнного стану та гібридних атак, ІССП МВС України стають першочерговими цілями для кібератак кіберзлочинців, особливо державних акторів рф. З метою нейтралізації таких загроз у системі «ІПНП» передбачено здійснення низки заходів. Зокрема, адміністратор системи «ІПНП» забезпечує облік користувачів і надання їм доступу до наявної інформації. Він також відповідає за захист інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом здійснення організаційних і технічних заходів, упровадження засобів і методів технічного захисту

---

[1] Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів : постанова Кабінету Міністрів України від 14 листоп. 2018 р. № 10244. URL: https://zakon.rada.gov.ua/lows/en/1024-2018-%D0%BF#Text

[2] Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 3 серп. 2017 р. № 676. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text

[3] Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua /laws/show/580-19#Text

[4] П'яте місце в Європі. *Суспільне. Новини :* [сайт]. URL: https://suspilne.media/1141546-ukraina-posila-pate-misce-u-sviti-za-vidsotkom-kiberatak-proti-kraini-microsoft/

[5] Armageddon. *Державна служба спеціального зв'язку та захисту інформації України :* [сайт]. URL: https://cip.gov.ua/ua/news/rosiiske-ugrupuvannya-gamaredon-suttyevo-zbilshilo-kilkist-kiberoperacii-protevoni-ne-taki-uspishni-yak-ranishe

[6] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7

інформації. У цій системі основним засобом перевірки повноважень користувачів є ідентифікатор доступу – об'єкт з унікальним атрибутом, що ідентифікує суб'єкта (користувача) в системі «ІПНП» (логін і пароль), реалізований через механізм парольного доступу. Цей превентивний захід захисту спроможний попередити приблизно 50 % спроб несанкціонованого втручання. Отже, майже половина кібератак досягають своєї мети.

Тому виникає гостра потреба в комплексному аналізі способів здійснення кібератак, а також у розробленні ефективних методів захисту від них.

Матеріали та методи

У статтях В. А. Кудінова (2017; 2023) та К. В. Ярового (2023) наведено комплексний підхід щодо створення стійких паролів, який надасть можливість користувачам ІССП МВС і НПУ забезпечити високий рівень стійкості парольного захисту до перебору. У роботі В. А. Кудінова (2021) визначено окремі вимоги щодо створення та використання користувачами стійких паролів в інформаційних системах ІССП МВС і НПУ. Аналізу кіберзагроз в умовах стрімкого розвитку інформаційних технологій та осмисленню їх як кібертероризму присвячені статті О. В. Гайдука та В. П. Звєрєва (2024), а також Р. В. Бараненка (2021). Гібридні атаки й атаки на критичну інфраструктуру досліджено в роботах Ю. П. Калайди (2025) та Р. К. Мурасова, С. І. Фараона та О. М. Гука (2025). У публікаціях А. Шолойко (2023) та О. О. Летичевського (2023) сформульовано наукові проблеми кібербезпеки. Вивченню кібератак на корпоративні бази даних приділено увагу в роботах С. В. Легомінова, Ю. В. Щавінська, О. В. Будзинський (2024); Є. А. Дроздова, В. М. Козел (2025). Роль штучного інтелекту в підвищенні кіберстійкості окреслено в статті О. М. Лунгол (2024).

Наявні методичні підходи переважно фокусуються на протидії окремим видам загроз без урахування системних взаємозв'язків усередині ЄІС МВС України. Тобто комплексний підхід до системної нейтралізації різних типів сучасних кібератак на такі специфічні системи, як ІССП, досі залишається недостатньо дослідженим у вітчизняній науці, особливо в умовах воєнного стану. Ця робота спрямована на усунення цього недоліку.

Мета статті. Обґрунтування перспективних напрямів удосконалення кіберзахисту та підвищення загального рівня кіберстійкості ІССП МВС України в сучасних умовах.

Результати й обговорення

Кібератака – це умисна дія одного або кількох зловмисників (від окремих хакерів до організованих груп або навіть державних структур), спрямована на отримання несанкціонованого доступу, модифікацію, дестабілізацію, знищення або блокування цифрових ресурсів (даних, мереж, систем, пристроїв).

Сьогодні кібератаки стали не просто технічною проблемою, а реальною загрозою для державних установ. Згідно з доповіддю Світового економічного форуму (WEF) «Global Cybersecurity Outlook 2025» 72 % опитаних організацій повідомили про збільшення кіберризиків. Кіберзлочинці щодня вдосконалюють масовані кібератаки, зокрема використовуючи методи ШІ. Їхні дії ґрунтуються на вразливостях програмного забезпечення (далі – ПЗ) та людському факторі. Такі кібератаки спрямовані на системи, які використовують в інтересах національної безпеки, оборони, правоохоронних органів і критичної інфраструктури (Yakovlev, & Liubchak, 2023).

Дослідження передбачає аналіз ключових загроз від імовірних типів кібератак на відомчі інформаційні системи й обґрунтування рекомендацій щодо комплексного підходу до підвищення їхньої кіберстійкості.

І. Шкідливе програмне забезпечення (malware) та віруси-вимагачі

Це загальний термін для будь-якого коду або програм, створених для пошкодження пристроїв, викрадення даних або отримання несанкціонованого доступу. Віруси-вимагачі (ransomware) є окремим видом malware, який шифрує файли жертви або блокує доступ до системи, вимагаючи гроші (викуп) за їх відновлення (Antonenko, Dihtiar, & Krykun, 2022).

Основні види загроз:

– віруси та хробаки: поширюються через файли або мережі;

– троянські програми: маскуються під корисне ПЗ;

– шпигунське ПЗ (spyware): таємно збирає інформацію про користувача;

– рекламне ПЗ (adware): показує небажану рекламу.

Основні методи захисту від malware та ransomware

1. Встановіть антивірусне програмне забезпечення: а) використовуйте надійні антивірусні програми та регулярно оновлюйте їх; б) уникайте використання програм російського походження через ризик компрометації.

2. Регулярно оновлюйте ПЗ: операційну систему (Windows, macOS, Android, iOS) та всі встановлені програми, оскільки оновлення усувають вразливості, якими користуються хакери.

3. Створюйте резервні копії (Backup). Регулярно зберігайте важливі дані на зовнішніх носіях або в хмарних сховищах. Це єдиний надійний спосіб відновити дані, якщо вимагачі зашифрують їх.

4. Будьте обережні в Інтернеті: 1) не відкривайте підозрілі вкладення в електронних листах і не переходьте за невідомими посиланнями; 2) завантажуйте програми лише з

офіційних джерел (App Store, Google Play, офіційні сайти розробників).

5. Використовуйте двофакторну аутентифікацію (2FA). Це додатковий захист ваших облікових записів, що ускладнює доступ зловмисникам навіть під час отримання пароля.

II. Фішинг і цілеспрямований фішинг (spear phishing)

Фішинг (phishing) для ІССП МВС України становить критичну загрозу, оскільки метою зловмисників є не лише викрадення особистих даних, а й доступ до службової інформації, баз даних (наприклад, реєстри МВС, «Дія»), компрометація персоналу та дестабілізація роботи правоохоронних органів. З урахуванням гібридної агресії та підвищеного інтересу спецслужб рф до правоохоронних органів, захист ІССП потребує комплексного підходу: поєднанні жорстких технічних засобів, організаційних заходів і навчання персоналу (Yakovlev, & Liubchak, 2023).

Основні загрози (фішинг-сценарії):

– «судові повістки» та фейкові запити: розсилка шкідливих листів, що імітують офіційні документи, з метою змусити користувача відкрити вкладення або перейти за посиланням;

– Targeted Phishing (Цільовий фішинг/Spear Phishing): листи, спрямовані на конкретних працівників МВС, що містять «службові» теми (наприклад, «Терміновий наказ», «Оновлення доступу до системи»);

– Business Email Compromise (BEC): підробка електронних адрес керівництва для отримання термінової інформації;

– використання ШІ: створення реалістичних фішингових повідомлень українською мовою, які важко розпізнати;

– фейкові ресурси: імітація офіційних сайтів сервісних центрів МВС чи відомчих порталів для крадіжки логінів/паролів.

Основні методи захисту від фішингових кібератак

1. Технічні заходи (захист ІССП МВС базується на поєднанні технічних рішень і суворих процедур безпеки): 1) багатофакторна автентифікація (MFA): обов'язкова для всіх користувачів службових систем, що робить вкрадений пароль марним для зловмисника; 2) поштовий захист: використання систем фільтрації спаму та шкідливих вкладень, SPF/DKIM/DMARC протоколів для запобігання підробці доменів; 3) мережеві екрани й антивіруси: встановлення антивірусного ПЗ, фаєрволів (WAF) і систем виявлення вторгнень; 4) контроль зовнішніх носіїв: обмеження використання USB-накопичувачів; 5) оновлення ПЗ: своєчасне встановлення патчів безпеки на робочих станціях і серверах.

2. Організаційні заходи та навчання персоналу: 1) регулярні тренінги: навчання працівників розпізнавання фішингових повідомлень; 2) симуляція атак: проведення фіктивних фішингових розсилок для перевірки пильності персоналу; 3) чіткий протокол реагування: співробітники повинні негайно повідомляти ІТ-відділ про підозрілі листи, не натискаючи посилання.

Як розпізнати фішинг? Пам'ятка для співробітника: а) адреса відправника: перевіряйте домен (після @). Офіційні листи надходять тільки з gov.ua; б) терміновість/загрози: фішери змушують діяти швидко («Ваш акаунт буде заблоковано», «Терміново оновити дані»); в) підозрілі посилання: наводьте курсор на посилання, щоб побачити реальну адресу перед натисканням; г) помилки в оформленні: нетиповий стиль спілкування або помилки в офіційних листах.

У разі виявлення фішингу слід звертатися до Департаменту кіберполіції Національної поліції України.

III. Розподілені атаки на відмову в обслуговуванні (DDoS)

Це скоординована кібератака, під час якої величезну кількість запитів одночасно спрямовують на вебсайт, сервер або мережу з багатьох джерел. Головна мета – перевантажити ресурси системи настільки, щоб вона не могла обробляти запити справжніх користувачів, стаючи фактично недоступною.

Основні типи DDoS-загроз (атаки класифікують залежно від того, на який рівень мережевої моделі OSI вони спрямовані):

– об'ємні атаки (Volumetric): найпоширеніший вид, мета якого – повністю зайняти пропускну здатність інтернет-каналу. Сюди належать UDP-флуд та ICMP-флуд;

– протокольні атаки: спрямовані на вичерпання ресурсів мережевого обладнання (фаєрволів, балансувальників навантаження). Наприклад, SYN-флуд, що використовує вразливості встановлення TCP-з'єднання;

– атаки на рівні додатків (L7): найвитонченіші атаки, що імітують поведінку реальних користувачів (наприклад, HTTP-флуд). Вони спрямовані на конкретні функції сайту, які потребують значних обчислювальних витрат сервера.

Небезпечність DDoS-атак полягає у: а) масштабності: оскільки запити надсилаються з тисяч або мільйонів пристроїв (часто заражених вірусами гаджетів IoT, що утворюють ботнет), заблокувати таку атаку за однією IP-адресою неможливо; б) складності ідентифікації: справжнє джерело атаки приховане за розподіленою мережею проміжних пристроїв по всьому світу; в) наслідках: окрім фінансових втрат через простій бізнесу, атаки можуть слугувати «димовою завісою» для крадіжки даних або іншого шпигунства (Kremin, Kremin, & Mindzia, 2025).

Основні методи протидії на DDoS-загрози

Для протидії використовують спеціалізовані рішення, такі як:

1. Хмарні сервіси захисту (наприклад, від Microsoft або Cloudflare), які фільтрують трафік перед тим, як він потрапить на ваш сервер.

2. Моніторинг мережі для виявлення аномальних сплесків активності на ранніх етапах.

3. Налаштування брандмауерів та обмеження кількості запитів (Rate Limiting) для зменшення впливу дрібних атак.

IV. Внутрішні атаки (Insider Threats)

Внутрішні атаки (insider threats) – це загрози безпеці, що походять від людей, які мають легітимний доступ до активів організації: співробітників, підрядників або бізнес-партнерів. На відміну від зовнішніх атак, інсайдери вже перебувають усередині периметра захисту, що суттєво ускладнює виявлення їхніх дій (Hlazunov, & Hurzhii, 2025).

Типи внутрішніх загроз (фахівці класифікують інсайдерів за їхніми мотивами та поведінкою):

1. Недбалий працівник (The Careless User): найпоширеніший тип. Це люди, які випадково наражають компанію на ризик через помилки: перехід за фішинговими посиланнями, використання слабких паролів або надсилання конфіденційних листів не тому адресату.

2. Зловмисний інсайдер (The Malicious Insider): діє навмисно з метою викрадення даних, саботажу або отримання фінансової вигоди. Це може бути незадоволений працівник, який хоче помститися, або людина, яка продає корпоративні секрети конкурентам.

3. «Кріт» або зовнішній агент (The Pawn/Mole): співробітник, якого завербували або обманом змусили надати доступ до мережі зовнішнім зловмисникам чи іноземним розвідкам.

4. Скомпрометований користувач: легітимний працівник, чиї облікові дані були викрадені хакерами за допомогою шкідливого ПЗ або соціальної інженерії. Атака виглядає як дії співробітника, але виконується зовнішньою силою.

5. Третя сторона (The Partner): підрядники чи постачальники, які мають доступ до систем компанії, але не дотримуються належних стандартів безпеки, створюючи вразливості.

Методи захисту від внутрішніх атак

Ефективна стратегія захисту потребує поєднання технічних засобів та організаційних заходів:

1. Принцип найменших привілеїв (PoLP): надавайте співробітникам доступ лише до тих даних і систем, які критично необхідні для виконання їхніх безпосередніх обов'язків.

2. Використання DLP-систем (Data Loss Prevention): спеціалізоване програмне забезпечення, що відстежує та блокує несанкціоновану передачу конфіденційної інформації за межі компанії.

3. Аналіз поведінки (UEBA): інструменти, які використовують машинне навчання для виявлення аномальної активності (наприклад, копіювання великих обсягів даних у неробочий час).

4. Багатофакторна автентифікація (MFA): обов'язковий захід, що значно ускладнює використання викрадених паролів.

5. Моніторинг і логування: постійний аудит дій привілейованих користувачів та адміністраторів систем.

6. Навчання персоналу: регулярні тренінги з кібергігієни для запобігання випадковим витокам через недбалість.

7. Процедури звільнення: чіткий регламент миттєвого блокування всіх доступів після припинення співпраці з працівником.

V. Експлуатація вразливостей (Exploiting Vulnerabilities)

Використання «дірок» у ПЗ, які ще не були закриті патчами безпеки. Експлуатація вразливостей – це використання помилок або недоліків у коді програм, операційних систем чи апаратному забезпеченні для виконання несанкціонованих дій.

Основні типи вразливостей (вразливості часто класифікують за місцем їх виникнення та характером впливу):

– переповнення буфера (Buffer Overflow): запис даних поза межами відведеного обсягу пам'яті, що дає змогу зловмиснику змінити перебіг виконання програми;

– ін'єкції (Injections): упровадження шкідливого коду в запити до баз даних (SQL Injection) або команд ОС;

– міжсайтовий скриптинг (XSS): вбудовування шкідливих скриптів у вебсторінки, які переглядають інші користувачі;

– порушення автентифікації та авторизації: слабкі паролі, відсутність двофакторної автентифікації або помилки в логіці перевірки прав доступу;

– неправильна конфігурація: відкриті порти, стандартні налаштування за замовчуванням або відсутність необхідних обмежень доступу;

– вразливості нульового дня (Zero-day): недоліки, про які розробник ще не знає і для яких ще не випущено патчів.

Методи експлуатації (для реалізації атак використовують експлойти – спеціальні фрагменти коду або інструменти): а) розвідка: пошук відомих вразливостей через бази даних, такі як MITRE CVE (Common Vulnerabilities and Exposures); б) доставка: надсилання експлойту через фішингові листи, шкідливі вебсайти або через мережеве з'єднання; в) виконання: запуск коду для отримання доступу, викрадення даних або поширення вірусів.

Методи захисту від експлуатації вразливостей

Захист має бути комплексним і багаторівневим:

1. Керування вразливостями (Vulnerability Management): регулярне сканування систем на наявність дір і пріоритетне їх усунення.

2. Оновлення та патчинг: своєчасне встановлення оновлень безпеки від розробників ПЗ.

3. Використання VBS і HVCI: технології ізоляції на основі віртуалізації у Windows, які захищають цілісність коду ядра.

4. Безпечна розробка (DevSecOps): статичний аналіз коду (SAST) і тестування на проникнення на етапі створення програм.

5. Захист облікових даних: використання складних паролів, хешування та багатофакторної автентифікації.

VI. Атаки на вебдодатки (SQL-ін'єкції, XSS)

Атаки на вебдодатки – це спроби зловмисників використати вразливості в коді сайту для викрадення даних або отримання контролю над системою. Найпоширенішими є SQL-ін'єкції та XSS (Tereshchenko, Tereshchenko, & Chernysh, 2024).

1. SQL-ін'єкції (SQL Injection).

Це впровадження шкідливого SQL-коду в запити до бази даних через поля введення. Механізм: зловмисник вводить спеціальні символи (наприклад, ' OR '1'='1) у поле логіна, що змушує сервер виконати незаплановану команду.

Типи SQL-ін'єкції:

– класична (In-band): результат атаки одразу відображається на тій самій сторінці;

– сліпа (Blind): сервер не виводить помилок, тому хакер аналізує відповіді системи (так/ні) або затримки в часі;

– позасмугова (Out-of-band): дані виводяться через інший канал (наприклад, HTTP-запит до сервера хакера).

Методи захисту від SQL-ін'єкції:

1. Параметризовані запити (Prepared Statements): розділення коду SQL і даних користувача.

2. Валідація та фільтрація: перевірка, чи відповідають введені дані очікуваному формату (наприклад, тільки цифри для ID).

3. Принцип найменших привілеїв: користувач бази даних повинен мати доступ лише до тих таблиць, які йому необхідні.

2. Міжсайтовий скриптинг (XSS).

Упровадження шкідливого JavaScript-коду, який виконується в браузері іншого користувача. Механізм: браузер не може відрізнити код розробника від коду хакера, тому виконує все, що є на сторінці.

Типи XSS:

– збережена (Stored XSS): скрипт зберігається на сервері (наприклад, у коментарі) і спрацьовує у кожного, хто відкриє цю сторінку;

– відбита (Reflected XSS): шкідливий код передається через URL-параметри й одразу відображається на сторінці (часто використовується у фішингових листах);

DOM-based XSS: вразливість, що реалізується виключно в клієнтському JavaScript-коді.

Методи захисту від XSS:

1. Екранування (Output Encoding): перетворення символів типу < на <, щоб браузер сприймав їх як текст, а не код.

2. Content Security Policy (CSP): спеціальний заголовок сервера, який дає змогу виконувати скрипти лише з довірених джерел.

3. HttpOnly Cookie: заборона доступу JavaScript до сесійних файлів cookie.

Загальні методи захисту:

1. Web Application Firewall (WAF): спеціальний екран, що аналізує трафік і блокує підозрілі запити ще до того, як вони потраплять до програми.

2. Регулярне оновлення: використання актуальних версій фреймворків і бібліотек, де вразливості вже виправлені розробниками.

VII. Атака «Людина посередині» (Man-in-the-Middle – MitM)

Перехоплення інформації між користувачем (наприклад, поліцейським) і сервером, що дає змогу шпигувати за переданими даними. Це вид кіберзагрози, коли зловмисник таємно перехоплює та, можливо, змінює зв'язок між двома сторонами (наприклад, поліцейським і сервером), що надає можливість шпигувати за переданими даними.

Основні типи MitM-атак:

– перехоплення Wi-Fi (Evil Twin): хакер створює відкриту Wi-Fi точку з назвою, схожою на відому (наприклад, «Free_Hotel_WiFi»). Коли користувач підключається, весь ваш трафік проходить через пристрій нападника;

– ARP Spoofing: зловмисник надсилає фальшиві ARP-повідомлення в локальній мережі, щоб пов'язати свою MAC-адресу з IP-адресою шлюзу (роутера). Це дає змогу перехоплювати дані всередині мережі;

– DNS Spoofing (отруєння кешу): користувача переспрямовують на підроблений сайт замість справжнього (наприклад, замість вашого банку користувач потрапляє на його копію), змінюючи записи в DNS-системі;

– HTTPS Spoofing / SSL Stripping: нападник змушує браузер перейти з безпечного протоколу https:// на вразливий http://, що надає можливість бачити логіни та паролі у відкритому вигляді;

– викрадення сесії (Session Hijacking): крадіжка файлів cookie, які дають змогу хакеру зайти у ваш обліковий запис без введення пароля, оскільки сервер «впізнає» його як авторизованого користувача (Shkitov, Buzoveria, & Stadnichenko, 2024).

Основні методи захисту від MitM-атак:

Для звичайних користувачів:

1. Використовуйте VPN: це створює зашифрований тунель, через який нападник не зможе прочитати ваші дані, навіть якщо перехопить їх у публічному Wi-Fi.

2. Перевіряйте HTTPS: завжди звертайте увагу на «замочок» в адресному рядку. Використовуйте розширення типу *HTTPS Everywhere*.

3. Уникайте відкритих Wi-Fi: не проводьте банківські операції через публічні мережі. Якщо це необхідно, використовуйте мобільний Інтернет.

4. Двофакторна автентифікація (2FA): навіть якщо хакер дізнається пароль, він не зможе увійти без другого фактора (коду з SMS або додатка).

Для власників сайтів та адміністраторів:

1. HSTS (HTTP Strict Transport Security): налаштування, яке забороняє браузерам відкривати сайт через незахищений протокол HTTP.

2. Використання надійних сертифікатів SSL/TLS: регулярне оновлення протоколів до останніх версій (TLS 1.3) https://is.gd/eYb4at.

3. Сегментація мережі: ізоляція критичних вузлів мережі для запобігання поширенню атаки всередині системи.

VIII. Атаки на паролі (Brute Force)

Атаки методом «грубої сили» (brute force) – це спосіб зламу, за якого зловмисники систематично перебирають усі можливі комбінації символів, щоб вгадати пароль або ключ шифрування. Метою є облікові записи адміністраторів або користувачів, які мають високий рівень доступу.

Типи атак (Brute Force):

– проста атака (Simple Brute Force): автоматизований перебір комбінацій символів (літер, цифр, знаків) без використання спеціальних списків;

– словникова атака (Dictionary Attack): використання бази найпопулярніших або раніше викрадених паролів (наприклад, «123456» або «password»);

– гібридна атака: поєднання словникової атаки з варіаціями символів, наприклад, додавання цифр або спецсимволів до звичайних слів;

– Credential Stuffing: підставлення вже відомих пар «логін–пароль», які були викрадені з інших сервісів, оскільки користувачі часто використовують однакові дані всюди;

– зворотна атака (Reverse Brute Force): хакери беруть один популярний пароль і намагаються підібрати його до тисяч різних логінів (Dolia, E., & Dolia, O., 2026).

Методи захисту від атаки на паролі

Для ефективного протистояння перебору рекомендують комбінувати кілька рівнів безпеки:

1. Складність паролів: а) довжина від 12–16 символів; б) поєднання великих і малих літер, цифр та спеціальних знаків; в) унікальність – не використовуйте один пароль для різних сервісів.

2. Технічні обмеження (на боці сервісів): а) двофакторна автентифікація (2FA): навіть якщо пароль вгадано, зловмиснику знадобиться другий фактор (код з SMS, додатка або біометрія); б) обмеження спроб входу: тимчасове блокування акаунту або IP-адреси після 3–5 невдач; в) використання CAPTCHA: зупиняє ботів, змушуючи підтвердити, що діє людина.

3. Додаткові заходи: а) використання менеджерів паролів для генерації та надійного зберігання складних ключів; б) «соління» (salting): додавання випадкових даних до пароля перед його хешуванням у базі даних (для захисту від офлайн-перебору).

IX. Компрометація (Intrusion)

Втручання в роботу системи з метою зміни інформації, наприклад, дефейс (зміна зовнішнього вигляду) вебсайтів, що призводить до втрати конфіденційності, цілісності або доступності даних.

Основні типи компрометації:

– злам облікових записів: викрадення паролів через фішинг, брутфорс (перебір) або купівлю баз даних у DarkNet;

– експлуатація вразливостей: використання багів у ПЗ (наприклад, критичні вразливості в Windows або вебсерверах);

– шкідливе ПЗ (Malware): віруси, шифрувальники (Ransomware) та трояни, що дають віддалений доступ до системи;

– соціальна інженерія: маніпулювання персоналом для отримання доступу або конфіденційної інформації;

– внутрішня загроза: дії ображених або підкуплених співробітників компанії.

Методи захисту від компрометації

Щоб мінімізувати ризики, використовують концепцію ешелонованої оборони:

1. Автентифікація: обов'язкове впровадження MFA (багатофакторної автентифікації). Навіть якщо пароль вкрадуть, зловмисник не увійде без другого фактору.

2. Керування патчами: регулярне оновлення ОС і ПЗ для усунення вразливостей системи безпеки.

3. Мережевий захист: використання брандмауерів (Firewalls) та систем виявлення/ запобігання вторгненням (IDS/IPS).

4. Принцип найменших привілеїв: користувач повинен мати доступ лише до тих даних, які необхідні йому для роботи.

5. Моніторинг і логування: постійний аналіз системних журналів для виявлення аномальної активності на ранніх етапах.

6. Навчання персоналу: регулярні тренінги з кібергігієни для запобігання переходу співробітників за підозрілими посиланнями.

Дії, якщо компрометація вже сталася: а) ізоляція: відключити заражений пристрій від мережі; б) аналіз: з'ясувати шлях проникнення й обсяг викрадених даних; в) відновлення: зміна всіх паролів, очищення системи та відновлення даних із «чистих» бекапів.

Висновки

У сучасних умовах масованої гібридної агресії та перманентних кібератак на державний сектор забезпечення цифрової безпеки об'єктів критичної інфраструктури набуває стратегічного значення. Надійний захист інформаційних систем спеціального призначення МВС України потребує впровадження комплексного підходу, спроможного протидіяти синергетичним загрозам. Сформульовані в роботі рекомендації щодо вдосконалення відомчого кіберзахисту в умовах воєнного стану надають можливість мінімізувати

ризики компрометації даних і підвищити загальну кіберстійкість єдиної інформаційної системи МВС України.

Перспективи подальших досліджень у цьому напрямі пов'язані з обґрунтуванням специфіки кіберзахисту систем управління та зв'язку мобільних вогневих груп протиповітряної оборони, що функціонують у структурі МВС України.

Подяки

Немає.

Фінансування

Дослідження не фінансувалося.

Конфлікт інтересів

Немає.

References

[1] Antonenko, N., Dihtiar, Ya., & Krykun, N. (2022). Modern methods of combating computer viruses. *Economy and Society,* 43. DOI: 10.32782/2524-0072/2022-43-51

[2] Baranenko, R.V. (2021). Cyberattacks as one of the forms of cyberterrorism. *Informatics, computing and automation,* 32(71), 1(1), 45-50. DOI: 10.32838/2663-5941/2021.1-1/07

[3] Dolia, E.K., & Dolia, O.Ye. (2026). Reliability of authentication mechanisms in information systems: the influence of the human factor. *Bulletin of the Kherson National Technical University. Series "Information technologies",* 1(96), 250-259. DOI: 10.35546/kntu2078-4481.2026.1.34

[4] Drozdova, Ye.A., Kozel, V.M. (2025). Modern methods of database protection in conditions of cyber threats and war. *Bulletin of the Kherson National Technical University,* 3(94), 177-185. DOI: 10.35546/kntu2078-4481.2025.3.2.22

[5] Haiduk, O.V., & Zveriev, V.P. (2024). Analysis of cyber threats in the conditions of rapid development of information technologies. *Cybersecurity: education, science, technology,* 3(23), 225-236. DOI: 10.28925/2663-4023.2024.23.225236

[6] Hlazunov, A.S., & Hurzhii, A.M. (2025). Method for early detection of insiders in cloud environments. *Technical Engineering,* 2(96), 90-94. DOI: 10.26642/ten-2025-2(96)-90-94

[7] Kalaida, Yu.P. (2025). Hybrid cyberattacks in the context of Ukrainian-Russian cyberwar. *Information and Law,* 4(55), 206-214. DOI: 10.37750/2616-6798.2025.4(55).346481

[8] Kremin, I., Kremin, S., & Mindzia, O. (2025). DDOS attack on overflow of conntrack table. *Technical Sciences,* 1(347), 150-155. DOI: 10.31891/2307-5732-2025-347-20

[9] Kudinov, V.A. (2017). On the problem of creating reliable passwords for users of the Integrated Information and Search System of the Ministry of Internal Affairs of Ukraine. *Current problems of state information security management :* materials of the VIII scientific-practical conference (pp. 54-56). Kyiv: National Academician of the Security Service of Ukraine.

[10] Kudinov, V.A. (2021). General approach to creating and using reliable passwords for users of information systems. *Interdisciplinary research: scientific horizons and perspectives:* I International Scientific and Theoretical Conference (Vol. 2), (pp. 47-48). Vilnius, Republic of Lithuania: European Scientific Platform.

[11] Kudinov, V.A., & Yarovyi, K.V. (2023). A comprehensive approach to creating stable passwords for special-purpose information systems of the Ministry of Internal Affairs and the National Police of Ukraine (part 1). *Modern Special Equipment,* 3(74), 42-49. DOI: 10.36486/mst2411-3816.2023.3(74)

[12] Kudinov, V.A., & Yarovyi, K.V. (2023). A comprehensive approach to creating stable passwords for special-purpose information systems of the Ministry of Internal Affairs and the National Police of Ukraine (part 2). *Modern Special Equipment,* 4(75), 40-50. DOI: 10.36486/mst2411-3816.2023.4(75)

[13] Lehominova, S.V., Shchavinska, Yu.V., & Budzynskyi, O.V. (2024). Analysis of modern approaches to ensuring cybersecurity of corporate databases. *Modern Information Security,* 2(58), 50-58. DOI: 10.31673/2409-7292.2024.020006

[14] Letychevskyi, O.O. (2023). Modern scientific problems of cybersecurity. *Bulletin of the NAS of Ukraine,* 2, 12-20. DOI: 10.15407/visn2023.02.012

[15] Lunhol, O.M. (2024). Review of methods and strategies of cybersecurity using artificial intelligence. *Cybersecurity: education, science, technology,* 1(25), 379-389. DOI: 10.28925/2663-4023.2024.25.379389

[16] Murasov, R.K., Faraon, S.I., & Huk, O.M. (2025). Cybersecurity of critical infrastructure: assessment and management of cyberattack risks. *Modern Information Technologies in the Sphere of Security and Defence,* 3(54), 75-83. DOI: 10.33099/2311-7249/2025-54-3-75-83

[17] Shkitov, A.A., Buzoveria, N.G., & Stadnichenko, O.A. (2024). Methodological matrix for preventing MITM attacks in strategic and civil infrastructures. *Methods and quality control devices,* 2(53), 137-146. DOI: 10.31471/1993-9981-2024-2(53)-137-146

[18] Sholoiko, A. (2023). Cybersecurity as a new goal of sustainable development. *Digital Economy,* III(91), 43-52. DOI: 10.34025/2310-8185-2023-2.90.01

[19] Tereshchenko, K.V., Tereshchenko, T.P., & Chernysh, Yu.O. (2024). Analysis of the problem of SQL injections in web applications. *CYBERSECURITY: education, science, technology,* 1(25), 177-199. DOI: 10.28925/2663-4023.2024.25.177199

[20] Yakovlev, M., & Liubchak, V. (2023). Possibilities of artificial intelligence in detecting and preventing phishing and cyberattacks. *Cybersecurity: education, science, technology,* 1(29), 298-309. DOI: 10.28925/2663-4023.2025.29.840

Список використаних джерел

[1] Антоненко Н., Дігтяр Я., Крикун Н. Сучасні методи боротьби з комп'ютерними вірусами. *Економіка та суспільство*. 2022. Вип. 43. DOI: 10.32782/2524-0072/2022-43-51

[2] Бараненко Р. В. Кібератаки як одна з форм кібертероризму. *Інформатика, обчислювальна техніка та автоматизація.* 2021. Т. 32 (71). Ч. 1. № 1. С. 45–50. DOI: 10.32838/2663-5941/2021.1-1/07

[3] Доля Е. К., Доля О. Є. Надійність механізмів автентифікації в інформаційних системах: вплив людського фактора. *Вісник Херсонського національного технічного університету. Серія «Інформаційні технології»*. 2026. № 1 (96). С. 250–259. DOI: 10.35546/kntu2078-4481.2026.1.34

[4] Дроздова Є. А., Козел В. М. Сучасні методи захисту баз даних в умовах кіберзагроз та війни. *Вісник Херсонського національного технічного університету*. 2025. №3 (94). С. 177–185. DOI: 10.35546/kntu2078-4481.2025.3.2.22

[5] Гайдук О. В., Звєрєв В. П. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. *Кібербезпека: освіта, наука, техніка*. 2024. № 3 (23). С. 225–236. DOI: 10.28925/2663-4023.2024.23.225236

[6] Глазунов А. С., Гуржій А. М. Метод раннього виявлення інсайдерів у хмарних середовищах. *Технічна інженерія*. 2025. №2 (96). С. 90–94. DOI: 10.26642/ten-2025-2(96)-90-94

[7] Калайда Ю. П. Гібридні кібератаки в умовах українсько-російської кібервійни. *Інформація і право.* 2025. № 4 (55). С. 206–214. DOI: 10.37750/2616-6798.2025.4(55).346481

[8] Кремінь І., Кремінь С., Міндзя О. DDOS атака на переповнення таблиці conntrack. *Технічні науки.* 2025. Вип. 1 (347). С. 150–155. DOI: 10.31891/2307-5732-2025-347-20

[9] Кудінов В. А. До проблеми щодо створення надійних паролів користувачів Інтегрованої інформаційно-пошукової системи МВС України. *Актуальні проблеми управління інформаційною безпекою держави* : матеріали VIII наук.-практ. конф. (Київ, 24 трав. 2017 р.). Київ : НА СБУ, 2017. С. 54–56.

[10] Kudinov V. A. General approach to creating and using reliable passwords for users of information systems. *Interdisciplinary research: scientific horizons and perspectives :* I International Scientific and Theoretical Conference (Vilnius, March 12, 2021). Vilnius, Republic of Lithuania: European Scientific Platform, 2021. Vol. 2. P. 47–48.

[11] Кудінов В. А., Яровий К. В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 1). *Сучасна спеціальна техніка.* 2023. № 3 (74). С. 42–49. DOI: 10.36486/mst2411-3816.2023.3(74)

[12] Кудінов В. А., Яровий К. В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 2). *Сучасна спеціальна техніка.* 2023. № 4 (75). С. 40–50. DOI: 10.36486/mst2411-3816.2023.4(75)

[13] Легомінова С. В., Щавінська Ю. В., Будзинський О. В. Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних. *Сучасний захист інформації.* 2024. № 2 (58). С. 50–58. DOI: 10.31673/2409-7292.2024.020006

[14] Летичевський О. О. Сучасні наукові проблеми кібербезпеки. *Вісник НАН України*. 2023. № 2. С. 12–20. DOI: 10.15407/visn2023.02.012

[15] Лунгол О. М. Огляд методів та стратегій кібербезпеки засобами штучного інтелекту. *Кібербезпека: освіта, наука, техніка*. 2024. № 1 (25). С. 379–389. DOI: 10.28925/2663-4023.2024.25.379389

[16] Мурасов Р. К., Фараон С. І., Гук О. М. Кібербезпека критичної інфраструктури: оцінювання та управління ризиками кібератак. *Modern Information Technologies in the Sphere of Security and Defence.* 2025. № 3 (54). С. 75–83. DOI: 10.33099/2311-7249/2025-54-3-75-83

[17] Шкітов А. А., Бузоверя Н. Г., Стадніченко О. А. Методологічна матриця запобігання MITM-атакам у стратегічних та цивільних інфраструктурах. *Методи та прилади контролю якості.* 2024. № 2 (53). С. 137–146. DOI: 10.31471/1993-9981-2024-2(53)-137-146

[18] Шолойко А. Кібербезпека як нова ціль сталого розвитку. *Цифрова економіка*. 2023. Вип. III (91). С. 43–52. DOI: 10.34025/2310-8185-2023-2.90.01

[19] Терещенко К. В., Терещенко Т. П., Черниш Ю. О. та ін. Аналіз проблеми SQL-ін'єкцій в веб-застосунках. *КІБЕРБЕЗПЕКА: освіта, наука, техніка.* 2024. № 1 (25). С. 177–199. DOI: 10.28925/2663-4023.2024.25.177199

[20] Яковлев М., Любчак В. Можливості штучного інтелекту у виявленні та запобіганні фішингу й кібератакам. *Кібербезпека: освіта, наука, техніка*. 2023. № 1 (29). С. 298–309. DOI: 10.28925/2663-4023.2025.29.840

KUDINOV Vadym
PhD in Physical and Mathematical Sciences, Associate Professor, Head of the Department of Information Technologies, Educational and Scientific Institute of Law and Psychology of the National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-5299-0590;
TARASENKO Volodymyr
PhD in Physical and Mathematical Sciences, Associate Professor of the Department of Information Technologies, Educational and Scientific Institute of Law and Psychology of the National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
ORCID: https://orcid.org/0009-0005-0250-7678;
SHVETS Mykola
Lecturer of the Department of Information Technologies of the Educational and Scientific Institute of Law and Psychology of the National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-8489-4659

Directions for Improving Cyber Defense of Special-Purpose Information Systems of the Ministry of Internal Affairs of Ukraine in the Conditions of Martial Law

Abstract. In the conditions of martial law and ongoing hybrid aggression by the Russian Federation, Ukraine's information systems are subjected to about 15 targeted cyberattacks every day. During this period, critical infrastructure facilities of the state become particularly vulnerable, among which special-purpose information systems (SPIS) of the Ministry of Internal Affairs of Ukraine occupy a significant place. The mentioned departmental resources provide continuous information and analytical support for the daily activities of law enforcement agencies, units of the National Police of Ukraine, and emergency rapid response services. Despite the significant number of available scientific works in the field of information protection, a comprehensive approach to the systematic neutralization of various types of modern cyberattacks on such specific systems still remains insufficiently researched in domestic science. Existing methodological approaches mainly focus on countering individual types of threats, without taking into account systemic interconnections within the unified information system of the department. The purpose of the article is to substantiate promising areas for improving cyber defense and increasing the overall level of cyber resilience of the ISSP of the Ministry of Internal Affairs of Ukraine in modern conditions. The study conducted a detailed analysis of key threats arising from probable types of cyberattacks on departmental information systems, as well as the most critical vulnerabilities of existing security circuits were identified. Based on the analytical data obtained, a comprehensive approach to increasing their cyber resilience was proposed. Practical recommendations have been formulated to minimize the negative impact of cyber incidents on the overall level of security of special-purpose information systems of the Ministry of Internal Affairs of Ukraine, which will allow increasing the resilience of the units to cyber threats.

Keywords: cybersecurity; cyber resilience; critical infrastructure facilities; special-purpose information systems; Ministry of Internal Affairs of Ukraine; National Police of Ukraine; cyberattack; information protection.