СИТУАЦІЙНИЙ ЦЕНТР ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СБУ

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

ОБСЄ Організація з безпеки і співробітництва в Європі

НАЦІОНАЛЬНА РАДА УКРАЇНИ З ПИТАНЬ ТЕЛЕБАЧЕННЯ І РАДІОМОВЛЕННЯ

РАДА ВЕРХОВНА РАДА УКРАЇНИ Комітет Верховної Ради України з питань свободи слова

ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ

«ІНТЕРНЕТ-РЕСУРСИ»

РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА

ЧАСТИНА ІІІ

2025

Кібератаки на українські медіа

За три роки повномасштабної війни медіасектор опинився серед пріоритетних цілей агресора. За цей період зафіксовано понад 120 кібератак на сайти українських медіа, однак практика свідчить, що реальна кількість у рази більша.

Безрезультатні кібератаки досить часто не фіксуються й не завжди отримують належної уваги. Попри це, українські медіа щодня стикаються з різними формами кібервпливу з боку підконтрольних росії хакерських угруповань, навіть якщо вони не призводять до безпосередніх кіберінцидентів.

Вітчизняні редакції не завжди повідомляють відповідних суб'єктів забезпечення кібербезпеки про спроби атак, що ускладнює їх фіксацію, а головне – не дає можливості своєчасно реагувати на зміну тактик хакерських груп і ефективно протидіяти російським кібероперація̈м.

Атаки спрямовуються як на національні, так і на регіональні онлайн видання, що виконують суспільно важливу функцію інформування громадськості. У більшості випадків вони збігаються з критичними політичними, військовими або суспільно значущими подіями.

Форми атак варіюються: від масових спроб блокування інформаційних ресурсів до цілеспрямованих зламів редакційних систем і публікації дезінформаційних матеріалів, покликаних підірвати довіру суспільства до українських медіа.

Цілі атак

Кібератаки на українські медіа мають комплексний характер, поєднуючи технічні засоби впливу з інформаційно-психологічними методами. Їхня головна мета – послабити інформаційну стійкість України та підірвати довіру суспільства до власних медіа.

Основні цілі таких атак полягають у:

- дестабілізації медіапростору;
- підриві довіри громадян до незалежних джерел інформації;
- дискредитації журналістів, редакцій і медіаорганізацій;
- спотворенні публічного дискурсу та нав'язуванні ворожих наративів;
- зриві інформаційних кампаній і спроможності швидко інформувати населення;

- маніпуляції журналістськими матеріалами;
- порушенні координації між медіа та державними/громадськими інституціями.

Дії зловмисників нерідко координуються з більш широкими кампаніями дезінформації, які ведуться у соціальних мережах або через проросійські інформаційні ресурси. Зазначене вкотре підтверджує застосування державою-агресором тактики інтеграції кібероперацій у стратегію гібридної війни проти України.

Вектори атак

1. DDoS-атаки (відмова в обслуговуванні).

Атака типу **Distributed Denial of Service (DDoS)** полягає в тому, що зловмисники генерують великий обсяг трафіку або запитів до серверу, що робить його недоступним для легітимних користувачів. Така атака не обов'язково передбачає витік даних; її мета – зупинка роботи сервісу, підрив довіри до ресурсу. Для медіа це особливо критично, адже сайт може бути головним каналом донесення інформації, і його недоступність створює інформаційний вакуум. Крім того, **DDoS**-атака може використовуватися як прикриття для інших, більш складних атак.

23 лютого 2022 року здійснено DDoS-атаку на українське медіа «Українська правда»; у січні 2024 року – на медіа «ПРАВДА»; у серпні 2025 року – на сайт «Детектор медіа».

LIGA.net зазнає систематичних спроб злому: видання посилює кіберзахист

Після хвиль DDoS-атак зловмисники змінили тактику і тепер намагаються проникнути у внутрішні системи LIGA.net

Редакція LIGA.net

2. Фішинг/соціальна інженерія.

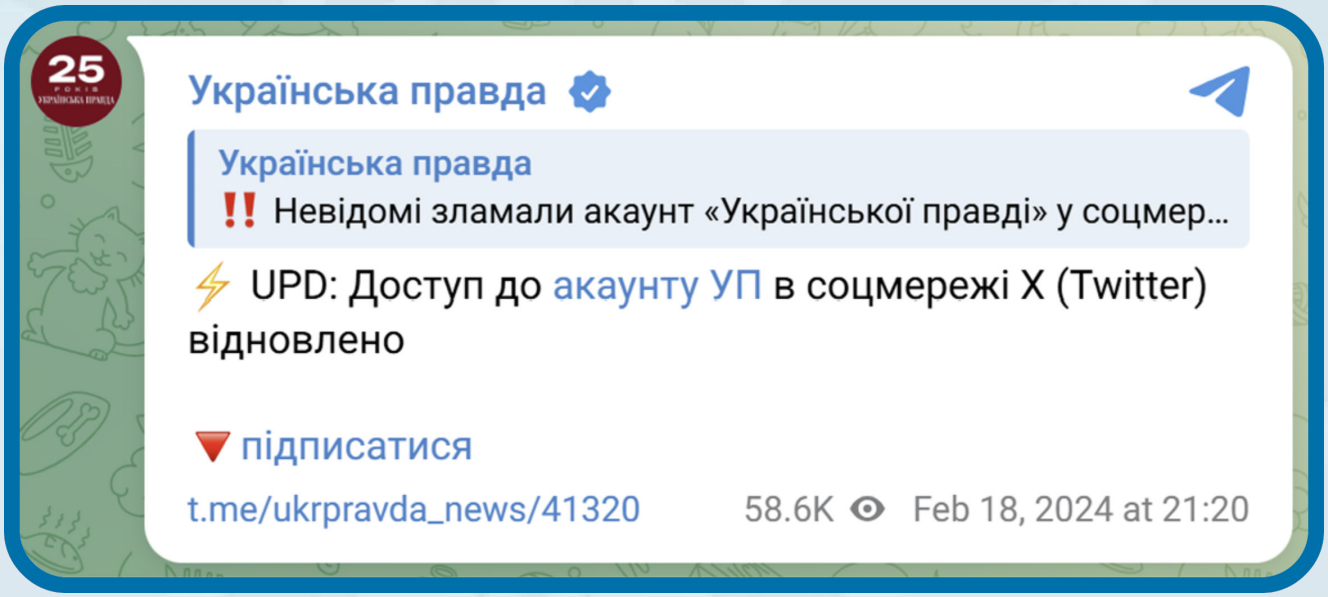
Цей тип атак спрямований на вивідування у користувачів чи працівників (журналістів, редакторів, адміністраторів) відомостей, які в подальшому дозволять отримати несанкціонований доступ до облікового запису, ресурсу, системи чи змусити завантажити шкідливе ПЗ, передати логіни/паролі тощо. Як приклад: лист-підробка від нібито відомого джерела з повідомленням чи вимогою «змінити пароль» або примусити здійснити перехід на підставний сайт.

«Інститут масової інформації отримав фішингові листи від хакерів, пов'язаних зі спецслужбами РФ», «Журналістка МикВістей отримала фішингове запрошення на вигаданий захід з НАТО та ЗСУ».

3. Компрометація облікових даних.

Ситуація, коли зловмисник отримує доступ до облікових записів журналістів, редакторів або до адміністративних доступів (**CMS, FTP/SFTP, SSH,** панелі хостингу, поштові скриньки тощо). Часто – це результат порушення правил кібергігієни, але також може бути й наслідком інших цілеспрямованих атак.

18 лютого 2024 року медіа «Українська правда» втратила доступ до свого акаунту в соцмережі X, і з нього були розміщені фейкові пости.



4. Використання вразливостей ПЗ та серверного обладнання.

Під час здійснення атак цього типу зловмисники експлуатують технічно слабкі місця: застаріле або неоновлене програмне забезпечення (**CMS, бібліотеки, плагіни**), помилки в налаштуваннях серверних служб (**FTP/**

SFTP, SSH) та недоліки мережевої конфігурації. Через такі вразливості зловмисники можуть проникнути в інфраструктуру, підвищити свої привілеї, встановити шкідливе ПЗ, підмінити або знищити контент і викрасти дані.

5. Дефейс або підміна контенту.

Атака передбачає зміну контенту ресурсу та оприлюднення на ньому фейкових повідомлень чи зміненого інформаційного контенту, який дискредитує медіа чи вводить аудиторію в оману. Дефейс часто спрямований на поширення паніки, підрив довіри до влади, загострення соціально-політичної ситуації в державі, інформаційний хаос.

Російські хакери здійснили чергову атаку на низку українських медіа та розмістили на їхніх ресурсах фейкову інформацію.

6. Постачальники послуг.

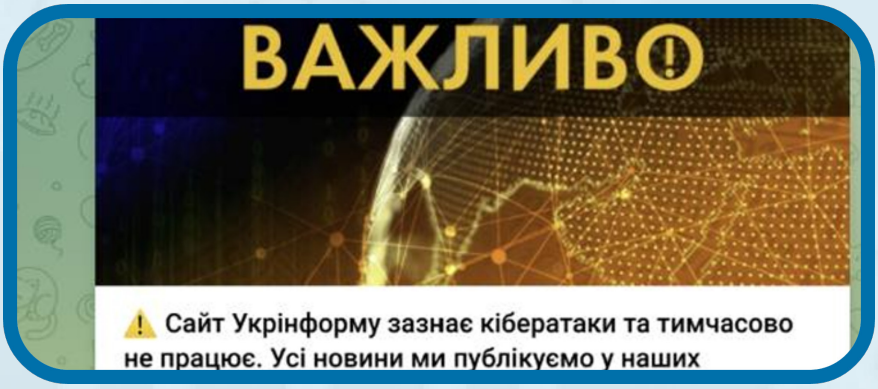
Медіа часто недостатньо контролюють свою інфраструктуру: вони користуються послугами хостингу, реєстраторів доменних імен, розробників вебсайтів та аутсорс-адміністрування своїх ресурсів. Ці підрядники мають привілейовані права (**доступ до серверів, панелей управління, DNS, механізмів оновлення, FTP/SFTP**). Компрометація будь-якого з таких постачальників відкриває зловмисникам шлях до ресурсів усіх клієнтів одночасно.

Російські хакери скористалися вразливостями в рекламній мережі RedTram, щоб розмістити символіку воєнних злочинців на сайтах українських медіа.

7. Знищення даних.

Деструктивні атаки – цілеспрямовані втручання в інформаційні системи з використанням шкідливого ПЗ типу wiper, спрямовані на повне або часткове руйнування даних. На відміну від програм, які викрадають інформацію, вайпери знищують файли, роблять їх недоступними, що унеможливлює відновлення даних з носіїв інформації. Наслідки – втрата даних, простій сервісів та істотні репутаційні й фінансові збитки для організацій і медіа.

17.01.2023 року «CyberArmyofRussia_Reborn» провели атаку на інформаційно-комунікаційні системи Українського національного інформаційного агентства «Укрінформ».



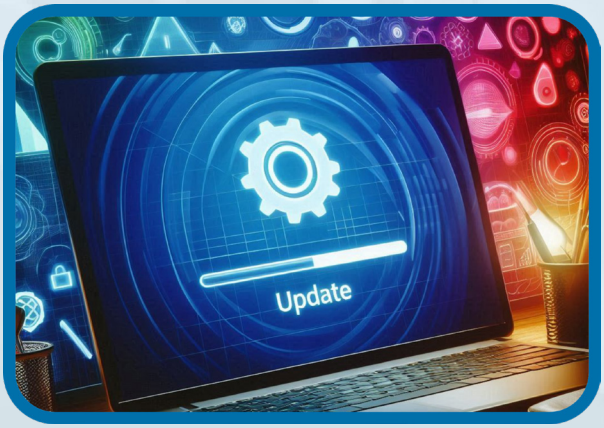
ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

Рекомендації для технічного адміністратора медіасайту

Превентивні заходи: для вебсайту

1. Оновлення програмного забезпечення.

Регулярно оновлювати **CMS**, плагіни, теми, серверне ПЗ (**ОС, вебсервер, базу даних**). Використовувати лише офіційні джерела та **LTS**-версії компонентів. Проводити тестування оновлень у середовищі staging. Активувати автоматичні повідомлення про критичні оновлення безпеки.



2. Управління обліковими записами та автентифікацією.

Необхідно впровадити політику складних паролів, їх регулярну зміну та обов'язкову двофакторну автентифікацію (**MFA**) для всіх користувачів із правами доступу. Забороняється спільне використання акаунтів. Неактивні облікові записи слід видаляти або деактивувати. Під час реєстрації користувача має застосовуватись додатковий підтверджувальний фактор (електронна пошта або номер телефону) з метою верифікації особи.

3. Контроль сторонніх компонентів.

Перед встановленням сторонніх модулів слід перевіряти їх на наявність уразливостей або шкідливого коду. Використовувати лише підтримувані рішення з високою репутацією. Заборонити встановлення плагінів із неофіційних джерел, а також зберігання надлишкових компонентів, що не використовуються для роботи Інтернет-ресурсу.

4. Резервне копіювання та відновлення.

Виконувати регулярне резервне копіювання (з однаковою частотою для файлів і баз даних), зберігати копії у фізично ізольованому середовищі. Щокварталу тестувати можливість повного відновлення з цих копій.

5. Сегментація прав доступу.

Дотримуватись принципу мінімальних привілеїв. Розмежувати ролі: журналісти – редагування та публікація, адміністратори – окремі облікові записи. Мінімізувати доступ з особистих пристроїв. За можливості – впровадити доступ до компонентів системи з визначених IP-адрес.

6. Сегментація мереж.

Розділити тестове, робоче та адміністративне середовища. Розмістити вебресурси, що мають доступ із мережі Інтернет, у **DMZ**-зоні. Для компонентів сайту застосовувати ізольовані віртуальні машини або контейнери. Внутрішні ресурси розміщувати в окремих підмережах для мінімізації ризику компрометації.

7. Контроль доступу до серверів.

Закрити всі непотрібні порти та обмежити протоколи/сервіси віддаленого доступу. Вимкнути публічний доступ до панелі адміністрування (зокрема для **WordPress: /xmlrpc.php, /wp-admin, /wp-login.php**). Для віддаленого адміністрування використовувати корпоративний **VPN** або архітектуру **Zero Trust**. Дозволяти **SSH**-доступ виключно за допомогою двоступеневої автентифікації **SSH** (криптографічний ключ + пароль).

8. Захист периметру.

Налаштувати **WAF** (**Web Application Firewall**), міжмережевий екран, блокувати IP-адреси відомих ботнетів і **C2**-серверів, перевіряти адреси щонайменше у 2–3 джерелах перед внесенням у блокліст (**AbuseIPDB, VirusTotal, OTX**). Використовувати механізми захисту від brute-force (**fail2ban, crowdsec**) та CAPTCHA.

9. Шифрування і протоколи безпеки.

Використовувати **TLS 1.3**, перенаправлення **HTTP-HTTPS, HSTS** (**HTTP Strict Transport Security**), а також заголовки: **Strict-Transport-Security, X-Frame Options, Content-Security-Policy, Referrer-Policy, X-Content-Type-Options**.

10. Контроль постачальників.

Обирати хостинг з ізоляцією середовищ, підтримкою виділених серверів і перевіреними політиками безпеки. Активувати **DNSSEC**, заблокувати можливість доменного трансферу, налаштувати **WHOIS Privacy Protection**.

11. Безпечна конфігурація вебсервера.

Приховати службові сторінки (**phpinfo.php, test.php**) і версії ПЗ, вимкнути непотрібні сервіси та виконання деяких системних команд **PHP/JAVA/ Python (system();, os.system();)**. Використовувати лише захищені методи доступу: **SFTP, SSH**.

12. Моніторинг і логування.

Увімкнути централізоване логування подій, зберігати логи поза веб-коренем. Використовувати систему моніторингу для відстежування стану серверів, мережевих ресурсів і безпеки (**Zabbix, Grafana**). Аналізувати журнали подій та налаштувати отримання алертів (**e-mail, Slack/Webhook**) на критичні інциденти та порогові значення (сплеск **POST**-запитів, численні 500/403, успішні підключення з підозрілих IP). Підозрілі запити можуть свідчити про несанкціоновані дії.

13. Періодична перевірка директорій.

Проводити аудит серверних директорій для пошуку вебшелів та бекдорів. Виявлення сторонніх файлів може свідчити про компроментацію систем.

14. Контент і публікації.

Передбачити обов'язкову модерацію редактором матеріалів перед публікацією та можливість застосування цифрового підпису автора чи редакції. Забезпечити автоматичний аналіз вмісту перед розміщенням, щоб запобігти впровадженню шкідливого коду, скриптів або payload-елементів у контент.

15. Регулярний аудит безпеки.

Проводити пентести, сканування вразливостей, перевірку плагінів і **DNS** записів, тестування відмовостійкості (наприклад, **DDoS**-тест).

Для поштового сервера

1. Налаштувати **SPF, DKIM, DMARC** для перевірки достовірності відправників.
2. Використовувати сервіси з антивірусом, антиспамом та sandbox (**Mail Security Gateway**).
3. Налаштувати TLS, MTA-STS, **reverse DNS**, заборонити **relay** без автентифікації.

4. Заборонити прийом вкладень із небезпечними розширеннями **ADE, ADP, .APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PSI, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH** тощо).

5. Створити окрему адресу для підозрілих листів, навчити співробітників передавати їх без відкриття.

6. Активувати **DNSSEC** для домену з метою захисту від підміни **DNS**-записів (**SPF, DKIM, MX**).

Реагування на кібератаку

- **DDoS-атака**: звернутись до хостинг-провайдера, активувати механізм **DoS mitigation** (**DDoS-захист через CDN, cloud-filtering**).
- **Компрометація акаунта**: негайно змінити пароль, відключити акаунт, перевірити активність, провести журналювання сесій, видалити підозрілу активність, примусово встановити **MFA**. Перевірити власний ПК на підозрілі файли/активність.
- **Вірус/шкідливе ПЗ**: ізолювати скомпрометовані вузли від мережі, зберегти та зафіксувати логи, провести сканування антивірусним програмним забезпеченням, відновити з резервної копії (попередньо перевірити бекапи на наявність ШПЗ), застосувати патчі та оновлення, змінити ключі/сертифікати.
- **Компрометація хостингу або домену**: зв'язатись із провайдером, змінити всі паролі, перевірити перенаправлення **DNS**, зафіксувати логи, звернутись до суб'єктів забезпечення кібербезпеки.
- **Після інциденту**: провести **root-cause** аналіз (аналіз першопричин), оновити політики, навчити команду, провести пост-інцидентний огляд і вдосконалити плани реагування.

Рекомендації для журналістів та редакцій

- Використовувати окремі акаунти для роботи та особистого користування.
- Активувати **MFA** на всіх сервісах: пошта, **CMS**, соцмережі.
- Не відкривати підозрілі листи чи вкладення; проходити навчання з кібергігієни.
-

- Регулярно змінювати паролі, використовувати менеджер паролів, вимкнути автозбереження у браузерах. Використовувати різні унікальні паролі для різних сервісів.
- Використовувати ліцензійне ПЗ, оновлену ОС, антивірус.
- Для чутливих комунікацій застосовувати VPN, зашифровану пошту, безпечні месенджери (**Signal, ProtonMail**).
- У разі підозри на злам – повідомити IT-службу, змінити паролі, припинити роботу до перевірки.
- Мати затверджений редакцією план реагування: алгоритм дій при атаці або компрометації акаунтів.

Рекомендації для власників та керівників медіа

- Включити заходи з кібербезпеки у стратегічне планування: виділений бюджет, відповідальні особи, політики безпеки.
- Проводити регулярне навчання журналістів і технічного персоналу із залученням експертів з кібербезпеки.
- Визначити вимоги безпеки у договорах із хостинг- та сервіс-провайдерами (резервування даних, відновлення, реагування на інциденти).
- Забезпечити відкриту комунікацію з аудиторією у разі атаки для збереження довіри.
- Регулярно аналізувати інциденти, оновлювати внутрішні політики.
- Забезпечити постійний моніторинг стану ресурсів і наявність плану аварійного відновлення (**DRP**).
- Призначити відповідальну особу (**CISO** / фахівця з інформаційної безпеки) або створити невелику групу безпеки для координації дій.

Рекомендації під час розробки сайту

1. Виконувати валідацію всіх полів вводу чи завантаження даних від користувачів, обмежувати типи завантажуваних файлів, зберігати їх поза веб-коренем.

2. Шифрувати чутливі дані, для паролів використовувати сучасні алгоритми хешування (**bcrypt** або **Argon2**).

3. Використовувати безпечні налаштування бази даних із TLS-з’єднаннями.

4. Не зберігати ключі автентифікації у коді.

5. Не виводити детальні повідомлення про помилки користувачам.

6. Виконувати регулярні перевірки безпеки протягом усього циклу розробки (**DevSecOps**).

7. Дотримуватись рекомендацій **OWASP Top 10**, **NIST SP 800-218 (SSDF)**.

8. Розмежовувати вебдодатки – ізолювати тестові або старі версії, щоб уразливості не загрожували основному ресурсу.

9. Перевіряти та видаляти метадані зображень (**EXIF**), щоб не зберігати GPS координати чи службову інформацію.

10. Використовувати мінімально необхідні права для кожного зовнішнього ключа чи токена.

Існує низка авторитетних джерел, що надають практичні рекомендації з безпечного проектування та налаштування вебресурсів. Найповніше ризики й способи їх мінімізації систематизовано в проекті **OWASP Top 10** – світовому стандарті для розробників, архітекторів і менеджерів із безпеки.

OWASP Top 10 узагальнює найпоширеніші вразливості вебдодатків, демонструє можливі сценарії їх експлуатації та пропонує ефективні методи запобігання. Це практичний орієнтир, що допомагає організаціям зменшити ризики кіберінцидентів і підвищити загальний рівень захищеності своїх цифрових платформ (**https://owasp.org/**).

Для повідомлення щодо протиправних дій у сфері інформаційної безпеки (Департамент кібербезпеки СБУ):

- E-mail: **cyber_security@dis.gov.ua**

Для невідкладного інформування про кіберінциденти та кібератаки (Ситуаційний центр забезпечення кібербезпеки СБУ)

- E-mail: **incident@dis.gov.ua**