https://doi.org/10.31891/2219-9365-2026-87-37
УДК 004.056.5:004.451

ІВАНЧЕНКО Євгенія
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0000-0003-3017-5752
e-mail: e.ivanchenko@duikt.edu.ua
ТУРОВСЬКИЙ Олександр
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0000-0002-4961-0876
e-mail: s19641011@ukr.net
РИЖАКОВ Микола
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0006-3377-7061
e-mail: nykolay.ryjakov@gmail.com

МЕТОДИКА ПОБУДОВИ СИСТЕМИ БЕЗПЕКИ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ДЛЯ РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

У статті розроблено ризик-орієнтовану методику побудови системи безпеки об'єкта інформаційної діяльності для роботи з інформацією з обмеженим доступом. Методика узгоджує системний контур кіберзахисту з фізичним та інженерно-технічним контуром об'єкта, охоплює класифікацію інформації, визначення меж довіри, аналіз ризиків, формування цільового профілю, реалізацію контролів, підготовку доказової бази, незалежне оцінювання, авторизацію та безперервний контроль. Запропоновано аналітичні показники притаманного і залишкового ризику, зваженого покриття вимог, повноти доказів та інтегральної готовності. Показано, що кількісні оцінки мають застосовуватися разом із блокуючими критеріями та експертною перевіркою. Практичне застосування продемонстровано на умовному сценарії обробки службової інформації; наведено матрицю відповідальності RACI та річну послідовність упровадження. Наукова новизна полягає у формалізації наскрізного зв'язку «ризик — вимога — реалізація — доказ — рішення про авторизацію» для системного та фізичного контурів ОІД. Результати придатні для планування впровадження, внутрішнього аудиту й підготовки до незалежного оцінювання. Запропоновані формули мають методичний, а не нормативний статус.

Ключові слова: об'єкт інформаційної діяльності; інформація з обмеженим доступом; система безпеки; аналіз ризиків; доказова база; цільовий профіль; авторизація; безперервний контроль.

IVANCHENKO Yevheniia, TUROVSKY Oleksandr, RYZHAKOV Mykola
State University of Information and Communication Technologies

METHODOLOGY FOR BUILDING A SECURITY SYSTEM FOR AN INFORMATION ACTIVITY FACILITY PROCESSING RESTRICTED INFORMATION

The article develops a risk-oriented methodology for building and operating a security system for an information activity facility that processes restricted information. The proposed approach integrates the cybersecurity perimeter of an information and communication system with the physical and engineering protection perimeter of the facility. The methodology covers information classification, inventory of assets and data flows, definition of trust boundaries, threat modelling, risk analysis, development of a target security profile, implementation of controls, evidence management, independent assessment, security authorization and continuous monitoring. Analytical indicators are introduced for inherent and residual risk, weighted coverage of target-profile requirements, completeness of verified evidence and overall readiness for assessment. The study emphasises that numerical scores must not replace professional judgement: an unfulfilled critical requirement, an unacceptable residual risk or the absence of mandatory evidence remains a blocking condition regardless of the aggregate index. The method is illustrated using a conditional system processing official information, including remote access, supplier support, backup and facility-protection scenarios. A RACI responsibility matrix and a twelve-month implementation sequence connect governance decisions with verifiable technical and organisational outcomes. The scientific contribution is the formalised end-to-end relationship "risk — requirement — implementation — evidence — authorization decision" applied simultaneously to logical, physical and engineering domains. The results can support project planning, internal audit, evidence preparation and continuous improvement. The formulas proposed in the article are methodological instruments and do not replace legally established assessment procedures or an organisation's approved risk-assessment methodology.

Keywords: information activity facility; restricted information; security system; risk analysis; evidence base; target security profile; security authorization; continuous monitoring.

Стаття надійшла до редакції / Received 11.06.2026
Прийнята до друку / Accepted 12.08.2026
Опубліковано / Published 10.09.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Виходячи з вимог законодавства та прийнятих систем класифікації відомо, що інформація з обмеженим доступом (ІзОД) охоплює конфіденційну, таємну та службову інформацію [1,2,3]. Об'єкт інформаційної діяльності (ОІД) — це приміщення, споруда або інший об'єкт, де здійснюється діяльність,

пов'язана з інформацією, що підлягає захисту [1,2,3]. Для практичного проєктування ці поняття слід розглядати разом, але не ототожнювати.

Система безпеки ОІД вирішує низку завдань, які охоплюють ідентифікацію, доступ, керування потоками даних, журналювання, резервування та реагування на кіберінциденти. Вказана система відносно ОІД визначає контрольовану зону, режим доступу до приміщень, розміщення технічних засобів та ризики витоку технічними каналами. Слабкість будь-якого контуру знижує результативність іншого.

Після набрання чинності Законом України № 4336-IX і затвердження постановою Кабінету Міністрів України № 712 порядків формування профілів та авторизації практична робота зміщується до керованого життєвого циклу ризиків, вимог, доказів та відповідальності [1–3].

Проблема полягає в тому, що цільовий профіль не можна сформувати лише з переліку засобів захисту. Він має описувати фактичну архітектуру, ролі, зовнішні сервіси, ОІД, ризики, параметри контролю, власників вимог і докази їх виконання.

Важливе уточнення. *Профільний підхід не скасовує спеціальних вимог до державної таємниці й технічного захисту інформації на ОІД. Конкретний склад робіт залежить від виду інформації, власника системи, призначення об'єкта та застосовних нормативних актів.*

Тому практична методика має поєднати чотири площини: правовий режим інформації, межі системи та ОІД, ризик-орієнтований вибір контролів і доказову готовність до оцінювання та авторизації.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Нормативну основу переходу до профільної моделі становлять Закон України № 4336-IX [1], порядок розроблення профілів і авторизації, затверджений постановою Кабінету Міністрів України № 712 [2], а також базові профілі для систем, у яких обробляється відкрита, конфіденційна або службова інформація [3, 4]. Порядок оцінювання стану кіберзахисту [10] визначає організаційний контекст незалежної перевірки, а методичні рекомендації Держспецзв'язку [14] деталізують формування цільового профілю. Водночас ці документи не дають єдиного прикладного алгоритму, який наскрізно поєднує кібернетичні, фізичні й інженерно-технічні заходи ОІД із матрицею доказів та показниками готовності. Саме ця методична прогалина визначає предмет дослідження.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є формування практичної методики побудови й експлуатації системи безпеки ОІД для роботи з ІзОД, яка пов'язує цільовий профіль із ризиками, реалізацією контролів, доказами, відповідальними та авторизаційними процедурами.

Для досягнення мети використано системний аналіз, декомпозицію життєвого циклу безпеки, моделювання ризику та готовності, порівняння системного й фізичного контурів, а також умовну апробацію методики на сценарії обробки службової інформації.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Методичний підхід до ризику та доказової готовності

Методологічне застереження. *Наведені нижче формули є авторським аналітичним інструментарієм для внутрішнього управління. Вони не встановлені Законом № 4336-IX, постановою № 712 чи базовими профілями і не замінюють затверджену в організації методику оцінювання ризиків.*

Ризик-орієнтований підхід потребує узгодженої шкали, за якою різні підрозділи однаково тлумачать ймовірність, вплив, ефективність контролю та залишковий ризик. Найпростіша модель використовує п'ятибальну шкалу ймовірності та впливу. Важливо не саме число, а обґрунтування оцінки та її зв'язок із конкретним активом, загрозою і бізнес-процесом.

Таблиця 1

Мінімальний словник аналітичної моделі

Символ	Зміст	Діапазон	Приклад доказу
L_i	Ймовірність реалізації сценарію i	1–5	Статистика інцидентів, дані моніторингу, експертна оцінка
I_i	Вплив на конфіденційність, цілісність, доступність і діяльність	1–5	BIA, оцінка збитків, критичність функції
E_i	Ефективність сукупності контролів для сценарію i	0–1	Випробування, журнали, результати аудиту
x_j	Ступінь виконання вимоги j	0–1	0 — не виконано; 0,5 — частково; 1 — підтверджено
w_j	Вага або критичність вимоги j	>0	Рішення власника ризику за затвердженою методикою

Оцінка притаманного ризику.

$$R_i = L_i \times I_i \quad (1)$$

R_i — ризик до врахування діючих контролів; L_i та I_i оцінюються за однаковою затвердженою шкалою.

Оцінка залишкового ризику.

$$R_{res,i} = R_i \times (1 - E_i) \quad (2)$$

E_i = 0 означає відсутність підтвердженого ефекту контролів, E_i = 1 — повне усунення ризику в межах моделі. На практиці значення 1 потребує особливо сильного обґрунтування.

Матриця допомагає швидко розставити пріоритети, але не повинна приховувати відмінності між сценаріями. Два ризики з однаковим добутком можуть мати різну природу: рідкісна катастрофічна подія потребує іншої стратегії, ніж часта подія з помірними наслідками. Тому до оцінки додають опис сценарію, власника, джерела даних, діючі контролі та строк перегляду.

Зважене покриття вимог цільового профілю.

$$C = \frac{\sum_{j=1}^{n} w_j x_j}{\sum_{j=1}^{n} w_j} \times 100\% \quad (3)$$

C показує не просто кількість закритих пунктів, а їхню вагу. Значення x_j фіксується лише після перевірки реалізації та доказу.

Повнота доказової бази.

$$D = \frac{N_{verified}}{N_{required}} \times 100\% \quad (4)$$

Nrequired — кількість обов'язкових доказів за цільовим профілем; Nverified — кількість доказів, які пройшли внутрішню перевірку актуальності, повноти та відтворюваності.

Приклад розрахунку. Для сценарію з L = 4 та I = 5 притаманний ризик становить 20. Якщо сукупна ефективність підтверджених контролів оцінена як E = 0,65, залишковий ризик дорівнює 20 × (1 − 0,65) = 7. Рішення про прийнятність оцінки 7 приймається за критеріями організації, а не лише за кольором матриці.

Вихідні дані та межі системи безпеки

Архітектура захисту починається з життєвого циклу інформації, а не з переліку технічних засобів. Для кожної категорії ІзОД визначаються джерело, автор, власник, одержувачі, місця створення й зберігання, канали передавання, допустимі перетворення, резервні копії, архів, строк зберігання та спосіб знищення. Окремо фіксуються паперові копії, друк, фотографування, голосове обговорення, тимчасові файли, журнали й телеметрія, які можуть містити фрагменти захищуваної інформації.

На кожному етапі діють різні ризики. Під час створення критичними є правильна класифікація й авторизація автора; під час передавання — автентичність адресата, захищений канал і неможливість непомітної підміни; під час використання — мінімальні повноваження, контроль експорту та захист робочого місця; під час зберігання — шифрування, резервування й фізична охорона; під час знищення — підтверджена незворотність і облік носія. Один контроль не може однаково ефективно покрити всі етапи.

Карта життєвого циклу повинна показувати переходи між доменами довіри. Дані можуть залишати захищену систему через API, електронну пошту, друк, резервну копію, канал підтримки, журнал, аналітичну платформу або мобільний пристрій. Кожний перехід описується як окремий сценарій: ініціатор, одержувач, протокол, шифрування, контроль цілісності, журналювання, строк, можливість відкликання і реакція на помилку.

Важливо врахувати метадані. Навіть якщо файл зашифрований, назва, адресати, час передавання, обсяг, IP-адреси або шаблон звернень можуть розкривати чутливий контекст. Цільовий профіль має охоплювати не лише зміст, а й телеметрію, ключі, конфігурації, журнали та резерви. Для кожного класу визначаються правила мінімізації й строк зберігання, щоб система не накопичувала дані без операційної потреби.

Інвентаризація повинна поєднати логічний і фізичний погляди. Логічний реєстр містить сервіси, компоненти, облікові записи, інтеграції, сховища, ключі, журнали й залежності. Фізичний реєстр охоплює приміщення, зони, стійки, робочі місця, мережеві траси, джерела живлення, засоби пожежогасіння, охоронну сигналізацію та пристрої, здатні створювати технічні канали витоку. Обидва реєстри мають використовувати спільні ідентифікатори активів.

Для кожного активу визначаються власник, адміністратор, місце розташування, версія, критичність, категорії даних, зовнішня експозиція, резервування і дата останньої перевірки. Невідомий актив не може бути належно захищений: він не отримує оновлення, не включається до журналювання, сканування й резервного копіювання. Тому процес виявлення має поєднувати CMDB, мережеве сканування, хмарні каталоги та фізичні обстеження.

ОІД описується через контрольовані зони й сценарії присутності. Для кожної зони визначаються допуск, супровід відвідувачів, облік ключів і карт, допустимі пристрої, правила фото- й аудіофіксації, технічне обслуговування, прибирання та дії після завершення робіт. Особлива увага приділяється суміжним

приміщенням, спільним інженерним мережам, вікнам, вентиляції, кабельним вводам і місцям тимчасового зберігання носіїв.

Інвентаризація не є разовим етапом. Новий віртуальний сервер, SaaS-сервіс, тестова база або точка Wi-Fi можуть з'явитися без формального проєкту. Автоматичне виявлення порівнюється з дозволеним реєстром; невідповідність породжує інцидент або заявку на легалізацію. Для фізичних активів проводяться регулярні звірки й обстеження, а переміщення обладнання погоджується з урахуванням меж ОІД і технічних каналів.

Межа довіри проходить там, де змінюється власник, рівень контролю, ідентичність, мережевий домен, фізична зона або правовий режим. Типові межі — між користувачем і прикладною системою, внутрішньою мережею та Інтернетом, основним майданчиком і хмарою, системою та постачальником, контрольованою зоною й загальнодоступним простором. Кожна межа повинна мати явний механізм автентифікації, авторизації, шифрування, журналювання та відмовостійкості.

Нульова довіра не означає відсутність довірчих відносин; вона означає, що довіра не надається лише через місце в мережі або попередній успішний вхід. Рішення про доступ враховує особу, пристрій, стан захисту, ресурс, контекст, час і ризик. Для ІзОД особливо важливі повторна перевірка привілейованих дій, короткострокові повноваження, ізольовані адміністративні робочі місця та розрив постійних довірчих зв'язків між середовищами.

Інтеграція розглядається як продукт із власником і життєвим циклом. API має каталог, схему даних, правила версіонування, автентифікацію, ліміти, журналювання, тестові сценарії та процедуру відкликання. Файловий обмін має контроль цілісності, захищений транспорт, карантин, антивірусну перевірку та підтвердження одержувача. Ручна передача через носій допускається лише за облікованою процедурою з перевіркою пристрою й незворотним очищенням.

Для критичних меж визначається безпечна відмова. Якщо недоступний сервіс ідентифікації, система не повинна автоматично відкривати доступ; якщо зупинилося журналювання, критичні операції або блокуються, або переходять у контрольований аварійний режим; якщо не підтверджено стан пристрою, користувач отримує лише мінімальний доступ. Сценарії відмови тестуються так само, як штатний доступ.

Модель загроз поєднує актив, суб'єкта, спосіб впливу, передумови, вразливість, наслідок і наявні контролі. Загальні списки загроз корисні як початкова перевірка, але цільовий профіль потребує конкретних сценаріїв: компрометація віддаленого адміністратора; викрадення резервної копії; підміна оновлення; несанкціоноване фото документа; підключення стороннього пристрою; витік через постачальника; зняття акустичної або електромагнітної інформації за межами контрольованої зони.

Таблиця 2

Приклади сценаріїв загроз для системи та ОІД

Сценарій	Передумова	Основний контроль	Доказ ефективності
Компрометація віддаленого доступу	Викрадений пароль або сесія	MFA, окремий шлюз, PAM, гео/ризик-політики	Тест входу, журнал блокування, вибірка сесій
Витік резервної копії	Копія доступна з основного домену	Ізоляція, шифрування, окремі ключі, immutability	Тест доступу й відновлення, журнал ключів
Підміна оновлення	Недовірений репозиторій або постачальник	Підпис, allowlist, SBOM, тестове середовище	Перевірка підпису, протокол розгортання
Несанкціонований пристрій в ОІД	Слабкий контроль відвідувачів/обладнання	Зонування, огляд, облік, технічне обстеження	Журнал допуску, акт обстеження
Акустичний витік	Мовна інформація виходить за контрольовану зону	Планування приміщень, режим, технічні заходи	Протокол вимірювань і перевірки
Зловживання адміністратором	Постійні надмірні повноваження	Розмежування, JIT, запис сесій, двоособове погодження	Вибірка привілеїв, журнал сесій

Для ОІД аналіз виходить за межі кіберзагроз. Враховуються акустичні, віброакустичні, електромагнітні та провідні канали, несанкціоновані пристрої, можливість візуального спостереження, спільні інженерні мережі, ремонтні роботи й тимчасовий персонал. Висновки обстеження впливають на зонування, розміщення робочих місць, конструктивні заходи, вибір обладнання і правила експлуатації.

Сценарій оцінюється не лише за ймовірністю атаки, а за доступністю передумов і спостережуваністю. Рідкісний, але непомітний канал із високим наслідком може вимагати пріоритету. Для кожного сценарію визначається профілактика, виявлення, локалізація, відновлення та доказ ефективності. Якщо контроль лише знижує ймовірність, але не виявляє реалізацію, додається незалежний механізм моніторингу.

Модель загроз переглядається після суттєвих змін, інцидентів і появи нових залежностей. Вона повинна бути зрозумілою власникам процесів: технічний опис доповнюється впливом на функції, строки,

юридичні обов'язки та репутацію. Це дає змогу керівництву приймати ризик усвідомлено й порівнювати витрати на контроль із реальними наслідками.

Організація роботи з інформацією з обмеженим доступом

1. Класифікувати інформацію до проєктування захисту

Перший документ проєкту — не перелік обладнання, а карта інформації. Необхідно визначити її власника або розпорядника, законну підставу обмеження доступу, категорію, місця створення, зберігання, передачі, резервування та знищення. Помилка на цьому етапі призводить до неправильного вибору профілю і може стати підставою для повернення авторизаційного листа на доопрацювання.

2. Проєктувати систему й ОІД як два взаємопов'язані контури

Системний контур охоплює ідентифікацію, доступ, сегментацію, криптографічний захист, журнали, резервування, моніторинг та реагування. Фізичний контур ОІД — контрольовану зону, пропускний режим, розміщення обладнання, інженерні мережі, захист мовної інформації, протидію технічним каналам витоку і контроль допоміжних технічних засобів. Слабкість будь-якого контуру знецінює інший.

3. Прив'язувати кожну вимогу до доказу

Для кожної дії цільового профілю варто заздалегідь визначити відповідального, технічну або організаційну реалізацію, параметр налаштування, періодичність контролю та доказ виконання. Доказом може бути політика, наказ, схема, конфігурація, журнал подій, протокол випробувань, запис навчання чи звіт про сканування. Це суттєво спрощує оцінювання та подальший аудит.

4. Вбудувати безпеку в експлуатацію

Авторизація не завершує проєкт. Потрібні процеси управління змінами, вразливостями, обліковими записами, носіями, резервними копіями, інцидентами та постачальниками. Якщо система модернізується, змінює архітектуру або профіль — перевіряється необхідність позапланової авторизації.

5. Не переносити ІзОД у зовнішній сервіс без моделі відповідальності

Хмарна інфраструктура, сервісний центр, віддалена підтримка або сторонній розробник не знімають відповідальності з власника системи. У договорі та цільовому профілі потрібно закріпити межі відповідальності, вимоги до доступу, журналювання, інцидентів, резервування, повернення або знищення даних і контролю субпідрядників.

6. Застосовувати принцип найменших повноважень до всього циклу даних

Обмеження доступу не зводиться до налаштування прав у прикладній системі. Потрібно охопити створення, погодження, друк, копіювання, експорт, пересилання, резервування, архівування та знищення інформації. Окремо перевіряються привілейовані облікові записи, аварійний доступ, сервісні облікові записи та тимчасові права підрядників. Для кожного винятку визначаються строк, власник і підстава.

7. Розглядати персонал і постачальників як елементи архітектури

Людина, сервісна організація або постачальник програмного компонента можуть мати більший вплив на ризик, ніж окремий технічний засіб. Тому до цільового профілю включають перевірку персоналу, навчання, правила поведінки, процедури переведення і звільнення, вимоги до розроблення, оновлення, повідомлення про вразливості та контроль субпідрядників. Договори мають підтримувати, а не суперечити моделі доступу й реагування.

Таблиця 3

Фрагмент матриці «вимога — реалізація — доказ»

Вимога	Реалізація	Доказ	Власник	Частота
Мінімізація привілеїв	Рольова модель, окремі адміністраторські облікові записи	Матриця ролей, експорт прав, протокол перевірки	IAM / IT	Щокварталу
Захист журналів	Централізований збір, розмежування доступу, контроль цілісності	Конфігурація SIEM, тест події, звіт про збереження	SOC	Постійно
Резервне відновлення	Ізольовані копії, контроль доступу, шифрування	Журнал копіювання, протокол тестового відновлення	IT-експлуатація	За графіком
Контроль ОІД	Контрольована зона, допуск, облік обладнання й інженерних змін	Акт обстеження, схеми, журнал відвідувань	Режимний підрозділ	Щороку / при зміні
Реагування на інциденти	Ролі, канали ескалації, сценарії локалізації та відновлення	План реагування, протокол навчання, картка інциденту	CSIRT / SOC	Не рідше разу на рік

Архітектура контролів і доказова база

Єдиний життєвий цикл ідентичності охоплює працівників, підрядників, сервісні облікові записи, обладнання й програмні компоненти. Джерелом істини для працівника є кадрова подія, для підрядника — договір і заявка власника, для сервісного запису — паспорт компонента. Створення, зміна та відкликання виконуються за вимірюваними строками; прострочена кадрова подія або завершений договір автоматично породжують блокування доступу.

Привілейований доступ відокремлюється від повсякденного. Адміністратор використовує персональний звичайний запис для роботи й окремий короткостроковий привілейований доступ для конкретної задачі. Сесія проходить через контрольований шлюз, записується, пов'язується із заявкою й перевіряється на аномалії. Аварійні записи зберігаються захищено, використовуються за двоособовим погодженням і негайно змінюються після застосування.

Шифрування даних під час передавання й зберігання ефективне лише за керованого життєвого циклу ключів. Визначаються генерація, активація, розподіл, зберігання, резервування, ротація, відкликання, знищення і дії при компрометації. Ключі не повинні зберігатися поруч із зашифрованими резервними копіями або в коді. Доступ до ключових операцій розмежовується, а критичні дії журналюються й, за потреби, вимагають двоособового контролю.

Вибір криптографічних засобів визначається правовим режимом інформації, моделлю загроз і нормативними вимогами. Самостійно створені алгоритми чи невідомі бібліотеки не можуть вважатися достатнім контролем. Цільовий профіль фіксує протоколи, мінімальні параметри, довірені центри, правила сертифікатів, заборонені конфігурації та процедуру оновлення. Автоматичний контроль виявляє прострочені сертифікати й слабкі параметри до виникнення відмови.

Архітектура журналювання починається з переліку контрольних запитань: хто отримав доступ; до яких даних; яку дію виконав; з якого пристрою; хто змінив права; чи було вимкнено захисний механізм; чи успішно виконано резервування; чи змінилася конфігурація. Для кожного питання визначаються джерела подій, обов'язкові поля, точність часу, строк зберігання, захист від зміни та правила кореляції.

Централізований збір не гарантує виявлення. Потрібні сценарії моніторингу, базові рівні, пороги, пріоритети й відповідальні за реакцію. Критичні сценарії перевіряються контрольними подіями: невдала MFA, додавання адміністратора, вимкнення агента, масовий експорт, звернення до резервної копії, запуск аварійного запису. Якщо подія не надходить або не створює потрібний сигнал, це невідповідність контролю.

RTO і RPO визначаються власником функції на підставі аналізу впливу, а не можливостей наявного обладнання. Для кожного сервісу описуються залежності: ідентифікація, DNS, ключі, мережа, постачальник, ОІД, живлення, журнали. Відновлення окремої бази не доводить відновлення послуги. Тест має пройти повний маршрут користувача, перевірити цілісність даних, права доступу та безпечну конфігурацію.

Копії ізолюються від основного домену адміністрування, шифруються, контролюються за незмінністю і регулярно перевіряються. Принаймні одна копія має бути захищена від масового видалення або шифрування. Тестові відновлення проводяться за різними сценаріями — випадкове видалення, компрометація, втрата майданчика, недоступність постачальника — і завершуються протоколом з фактичним часом, помилками та коригувальними діями.

Зовнішній сервіс включається до архітектури як залежний домен, а не як чорна скринька. Визначаються дані, адміністративні ролі, місця обробки, субпідрядники, механізми інтеграції, журнали, резервування, вихід із послуги та дії при інциденті. Докази постачальника перевіряються на релевантність конкретній конфігурації замовника; загальний сертифікат не підтверджує правильність ролей, ключів або журналювання тенанта.

Постачальник програмного забезпечення оцінюється за безпечним життєвим циклом розробки, керуванням залежностями, підписом оновлень, SBOM, процесом повідомлення про вразливості й строками виправлення. Канал оновлення є критичним контуром довіри. У продуктивному середовищі оновлення перевіряється, проходить тестування, може бути відкочене й розгортається з контролем цілісності.

Людський фактор включається до архітектури через ролі, перевірки, навчання, розмежування обов'язків і контроль змін статусу. Навчання має бути рольовим: користувач розпізнає ІзОД і правильно повідомляє про подію; адміністратор працює через PAM і зберігає доказ; розробник не включає секрети до коду; керівник приймає ризик на підставі сценарію й строку; працівник ОІД дотримується зонування та правил обладнання.

Фізичний контроль підтримує системний. Допуск до приміщення не повинен автоматично надавати доступ до всіх стійок, консолей або носіїв. Зони розділяються за критичністю, відвідувач супроводжується, дії технічного персоналу плануються, а аварійний доступ журналюється. Камери й системи контролю доступу також є інформаційними системами: їх журнали, час, резервування й повноваження мають бути захищені.

Постанова № 712 визначає послідовність, яка перетворює профіль на право експлуатації системи.[3]

Інвентаризація та визначення сфери. Фіксуються система, власник/розпорядник, види інформації, межі та взаємозв'язки.

Вибір базового або галузевого профілю. Рішення має відповідати виду інформації та функціональному призначенню.

Оцінка ризиків. Визначаються актуальні загрози, вразливості, наслідки й допустимий ризик.

Розроблення і затвердження цільового профілю. Мінімальні вимоги конкретизуються для архітектури та процесів організації.

Реалізація заходів. Впроваджуються технічні, криптографічні, організаційні та фізичні контролі.

Оцінювання дотримання цільового профілю. Кваліфікований суб'єкт перевіряє документи,

конфігурації, процеси й результати випробувань.

Авторизаційний лист і внесення до переліку. Після позитивного оцінювання дані подаються до Адміністрації Держспецзв'язку.

Таблиця 4

Доменна карта контролів і ключових доказів

Домен	Ключовий результат	Базові механізми	Сильний доказ
IAM/PAM	Лише належні особи мають мінімальний і своєчасний доступ	MFA, JIT, розмежування, recertification	Експорт ролей, запис сесій, протокол перегляду
Криптографія	Дані й ключі захищені протягом життєвого циклу	TLS, шифрування, HSM/KMS, ротація	Конфігурація, журнал ключів, тест компрометації
Моніторинг	Критичні події виявляються й обробляються	Централізовані журнали, SIEM, use cases	Контрольна подія та картка інциденту
Стійкість	Послуга відновлюється у визначені строки	Ізольовані копії, DR, резервні канали	Протокол повного відновлення
Постачання	Зовнішня залежність не створює некерований ризик	Договір, оцінка, SBOM, shared responsibility	Звіт перевірки й план усунення
ОІД	Контрольована зона й технічні канали відповідають ризику	Зонування, допуск, інженерні заходи	Акт обстеження, журнали доступу
Персонал	Ролі компетентні, перевірені й своєчасно змінюються	Навчання, SoD, кадрові тригери	Тест знань, вибірка joiner/mover/leaver

Первинна авторизація потрібна для початку експлуатації. Планова проводиться не пізніше ніж через один календарний рік після попередньої авторизації на підставі щорічного перегляду ризиків. Позапланова потрібна, зокрема, після змін базового, галузевого або цільового профілю; загальний строк її проведення — шість місяців від відповідної зміни, якщо інше не встановлено нормативним актом.

Таблиця 5

Види авторизації та управлінські тригери

Вид	Коли проводиться	Ключовий пакет	Контрольний строк / тригер
Первинна	До початку експлуатації системи	Цільовий профіль, результати оцінювання, авторизаційний лист та інші визначені документи	До введення системи в експлуатацію
Планова	Після попередньої авторизації	Щорічний перегляд ризиків, актуалізовані докази, результати повторного оцінювання	Не пізніше одного календарного року
Позапланова	Після суттєвих змін профілю, архітектури або інших визначених подій	Актуалізований профіль, аналіз змін і ризиків, оцінювання змінених заходів	Загалом у межах шести місяців від зміни, якщо не встановлено інше

Особливості захисту ОІД у межах нової моделі

Профільний підхід робить ОІД частиною загальної моделі ризику, але не замінює спеціальні роботи з технічного захисту. Практично це означає, що під час обстеження об'єкта слід одночасно відповісти на дві групи запитань.

Що відбувається всередині системи? Хто і з яких пристроїв входить, які потоки даних дозволені, як працюють журнали, резервні копії, оновлення, віддалене адміністрування та реагування на інциденти.

Що може вийти за межі контрольованої зони? Де озвучується ІзОД, які технічні засоби перебувають у приміщенні, які існують акустичні, віброакустичні, електромагнітні або провідні канали, хто має фізичний доступ і як контролюються зміни в інженерному середовищі.

Таким чином, нова «система безпеки ОІД» — це не окремий комплект обладнання. Це узгоджена сукупність режимних, організаційних, інженерно-технічних, програмних і криптографічних заходів, для яких визначені ризики, власники, параметри, докази та порядок постійного контролю.

Оцінювання готовності та безперервний контроль

Оцінювання готовності до незалежного оцінювання

Проєктній команді потрібен індикатор, який не підмінює незалежне оцінювання, але показує, де система ще не готова до нього. Для цього доцільно окремо вимірювати покриття профілю, повноту доказів, результати технічних випробувань, операційну сталість і готовність постачальників.

Таблиця 7. Компоненти індексу готовності

Ілюстративний індекс готовності до оцінювання.

$$A = 0.30C + 0.25D + 0.20T + 0.15O + 0.10S \quad (5)$$

Усі компоненти нормалізуються до шкали 0–100. Наведені ваги є прикладом; організація затверджує власні ваги з урахуванням критичності системи.

Приклад індексу. Якщо C = 82, D = 74, T = 90, O = 68, S = 60, то A = 77,3. Такий результат не означає автоматичної готовності: спочатку перевіряють, чи немає критичної невиконаної вимоги, яка повинна блокувати подання незалежно від середнього бала.

Зважений індекс зрілості процесів.

$$M = \sum_{k=1}^{m} \alpha_k m_k, \sum_{k=1}^{m} \alpha_k = 1 \quad (6)$$

m_k — оцінка зрілості окремого процесу (наприклад, доступи, зміни, інциденти, резервування); α_k — його вага. Індекс корисний лише разом із поясненням критеріїв кожного рівня зрілості.

Пріоритет усунення недоліків.

$$P_i = R_{res,i} \times K_i \times (1 + X_i) \quad (7)$$

K_i — коефіцієнт критичності функції, X_i — нормований показник зовнішньої експозиції. Модель піднімає у пріоритет недоліки, пов'язані з критичними функціями та зовнішньо доступними компонентами.

Таблиця 6

Компоненти індексу готовності

Показник	Зміст	Приклад вимірювання	Вага у прикладі
C	Покриття вимог цільового профілю	Зважена частка підтверджених вимог	30%
D	Повнота і якість доказів	Частка перевірених доказів без прострочення	25%
T	Технічні випробування	Успішні тести контролів, сканування, відновлення	20%
O	Операційна сталість	Доступи, зміни, інциденти, навчання, резервування	15%
S	Постачальники та зовнішні послуги	Договори, допуски, SLA, контроль субпідрядників	10%

Контрольний календар

Після авторизації система переходить до режиму доказової експлуатації. Для кожної вимоги визначається частота контролю: постійно, щодня, щотижня, щомісяця, щокварталу, щороку або за подією. Частота залежить від швидкості зміни ризику й здатності виявити відхилення. Привілейовані сесії та зупинка журналювання контролюються постійно; облікові записи — за кадровою подією і регулярно; відновлення — за графіком; профіль — щороку та після суттєвих змін.

Календар має власника, заміну, джерело даних, форму результату й строк ескалації. Невиконаний контроль не переноситься безслідно на наступний період: створюється відхилення з оцінкою ризику й коригувальною дією. Автоматизація зменшує ручну роботу, але сама також контролюється — перевіряються повнота джерел, успішність завдань, права сервісних записів і цілісність звітів.

Найцінніший календар поєднаний із процесами змін та інцидентів. Впровадження нового сервісу автоматично створює задачі для інвентаризації, журналювання, резервування, сканування та доказів. Інцидент запускає позапланову перевірку пов'язаних вимог. Прострочений сертифікат або невдале відновлення впливають не лише на операційну заявку, а й на оцінку ризику та готовності до авторизації.

Метрики без підміни змісту

Метрика повинна підтримувати рішення, а не створювати ілюзію точності. Відсоток виконаних вимог корисний лише з урахуванням ваги й блокуючих критеріїв. Середній строк усунення вразливостей не показує прострочену критичну вразливість на зовнішньому компоненті. Частка успішних резервних копій не підтверджує відновлення. Тому кожен агрегований показник доповнюється переліком критичних винятків і якісним поясненням.

Для запобігання маніпуляції визначення метрики фіксується до початку звітного періоду: чисельник, знаменник, джерело, виключення, частота й власник. Зміна методики відображається в історії, щоб не порівнювати несумісні періоди. Дані по можливості отримуються автоматично з первинних систем, а ручні коригування погоджуються й журналюються.

Рекомендовано поєднувати випереджальні та підсумкові показники. Випереджальні — охоплення MFA, актуальність доказів, частка протестованих сценаріїв, виконання навчань, строк відкликання доступу. Підсумкові — інциденти, простій, фактичне порушення RPO, повторні невідповідності. Якщо випереджальні метрики покращуються, а підсумкові ні, організація переглядає припущення про ефективність контролів.

Таблиця 7

Приклад календаря безперервного контролю

Контроль	Частота	Власник	Доказ	Тригер ескалації
Привілейовані сесії	Постійно/щоденний огляд	SOC/PAM	Записи й аналітичні сигнали	Непогоджена або невідтворювана сесія
Склад адміністраторів	Щомісяця та за кадровою подією	IAM	Експорт ролей і протокол	Невідомий/прострочений доступ
Вразливості	Щотижня/після зміни	Кіберзахист/IT	Звіт сканування й план	Критична експлуатована вразливість
Резервні копії	Щодня; відновлення щокварталу	Експлуатація	Журнал копіювання й протокол тесту	Порушення RPO або невдале відновлення
Докази профілю	Щомісяця	Власники вимог	Реєстр актуальності	Прострочений критичний доказ
Аналіз ризиків	Щороку та за суттєвою подією	Власник/кіберзахист	Затверджений звіт	Нова критична залежність або інцидент

Внутрішня перевірка доказової бази

Перед незалежним оцінюванням проводиться багаторівнева перевірка. Власник вимоги підтверджує реалізацію; контроль якості перевіряє належність, повноту, актуальність і відтворюваність; керівник ризику перевіряє, чи немає неприйнятного залишкового ризику; координатор авторизації формує індекс пакета й контролює версії. Одна особа не повинна виконувати всі ролі для критичних вимог.

Вибірка формується за ризиком: усі критичні компоненти, привілейовані ролі, зовнішні межі, випадки з інцидентами й винятками; для масових однорідних об'єктів — статистично або методично обґрунтована вибірка. Якщо один екземпляр не відповідає базовій конфігурації, команда визначає, чи це одиничний дефект, чи системна проблема процесу розгортання.

Результат пробного аудиту — не лише список недоліків, а карта причин. Недоліки групуються за управлінням, процесом, технологією, компетентністю, постачальником або доказом. Системна причина усувається централізовано; локальне виправлення одного сервера не закриває дефект базової конфігурації. Повторна перевірка виконується тим самим або сильнішим методом.

Зв'язок з оцінюванням стану кіберзахисту

Постанова № 1799 визначає організаційний контекст оцінювання стану кіберзахисту й дозволяє враховувати результати окремих видів оцінювання за встановлених умов [10] Для команди це означає можливість уникати дублювання, але не автоматично переносити будь-який звіт. Необхідно зіставити сферу, дату, методи, кваліфікацію оцінювача, версію системи та вимоги, які були перевірені.

Єдиний каталог доказів полегшує повторне використання результатів. Один технічний тест може підтверджувати кілька пов'язаних вимог, але зв'язки мають бути явними. Водночас не можна вважати один сертифікат універсальним доказом усіх контролів. Каталог зберігає первинний результат, методику, сферу, дату, обмеження й посилання на вимоги різних профілів або стандартів.

Практичне застосування методики

Призначити власника процесу. Закріпити відповідальність керівника, підрозділу кіберзахисту, IT, режимного та юридичного напрямів.

Провести інвентаризацію. Системи, ОІД, інформація, носії, інтеграції, підрядники, канали зв'язку й резервні копії.

Уточнити правовий режим даних. Визначити, що є відкритою, конфіденційною, службовою або таємною інформацією і на якій підставі.

Визначити межі системи та контрольованої зони. Зафіксувати компоненти, приміщення, зовнішні сервіси й точки переходу довіри.

Обрати належний профіль. Перевірити наявність галузевого профілю та спеціальних вимог.

Виконати аналіз ризиків. Оцінити кібернетичні, фізичні, кадрові, технічні та постачальницькі ризики.

Розробити цільовий профіль. Призначити заходи, параметри, відповідальних, докази й періодичність контролю.

Реалізувати й випробувати захист. Вести матрицю відповідності «вимога — реалізація — доказ — статус».

Організувати оцінювання та авторизацію. Заздалегідь перевірити кваліфікацію і незалежність оцінювача та повноту авторизаційного пакета.

Перейти до безперервного контролю. Календар ризик-аналізу, навчань, резервного відновлення, перевірок доступів, аудиту, планової авторизації.

Щоб дорожня карта не залишилася переліком побажань, відповідальність потрібно закріпити наказом або іншим внутрішнім рішенням. Практично зручно використовувати RACI: A — остаточно відповідальний за результат, R — виконавець, C — обов'язковий учасник консультацій, I — отримувач інформації.

Таблиця 8

Приклад розподілу відповідальності RACI

Робота	Керівник	Кіберзахист / ІБ	ІТ / експлуатація	Режимний та юридичний напрями
Визначення сфери та правового режиму	A	R	C	R/C
Аналіз ризиків	A	R	C	C
Розроблення цільового профілю	A	R	R	C
Захист ОІД і контрольованої зони	I	C	C	A/R
Реалізація технічних заходів	I	A/C	R	C
Збирання та перевірка доказів	I	A/R	R	C
Взаємодія з оцінювачем	A	R	C	C
Прийняття залишкового ризику	A	R/C	C	C

Приклад не є типовим рішенням. *Наведений сценарій і числові оцінки ілюструють логіку застосування формул. Реальна система потребує власної моделі загроз, обстеження ОІД, цільового профілю та підтверджених даних.*

Таблиця 10. Паспорт умовного сценарію

Для сценарію компрометації віддаленого доступу команда встановила L = 4 та I = 5, отже R = 20. Після впровадження MFA, окремого шлюзу, обмеження привілейованих ролей і централізованого журналювання ефективність сукупності контролів попередньо оцінили як E = 0,65. Розрахунковий залишковий ризик становить 7.

Однак число 7 приймається до роботи лише за наявності доказів: протоколу перевірки MFA, матриці ролей, тестового журналу події, підтвердження блокування непогодженого каналу та результату навчання персоналу. Якщо хоча б один критичний доказ відсутній, значення E переглядається в бік зменшення.

Далі команда розраховує покриття профілю C і повноту доказів D. Наприклад, високе покриття за кількістю вимог не компенсує відсутність протоколу відновлення або неврегульований доступ постачальника. Саме тому індекс готовності використовують разом із блокуючими критеріями: невиконана критична вимога, неприйнятний залишковий ризик або відсутність обов'язкового документа зупиняють подання на оцінювання.

Перший квартал створює основу: управління, класифікацію інформації, інвентаризацію системи й ОІД, схеми потоків, модель загроз, аналіз ризиків і вибір профілю. До кінця кварталу керівництво має затвердити сферу, критичні функції, цільові строки відновлення, власників вимог і пріоритети. Технічні швидкі покращення допускаються, якщо вони не суперечать цільовій архітектурі.

Таблиця 9

Паспорт умовного сценарію

Елемент	Вихідні умови	Основний ризик	Запланований контроль
Інформація	Службова інформація та супровідні відкриті дані	Помилкова класифікація і надмірне поширення	Реєстр категорій, маркування, правила експорту
Архітектура	Центральний сервіс, віддалені робочі місця, резервний майданчик	Компрометація віддаленого доступу	MFA, окремий шлюз, журналювання і сегментація
ОІД	Основне приміщення та зона технічного обслуговування	Несанкціонований фізичний доступ і технічні канали	Контрольована зона, допуск, облік обладнання, обстеження
Постачальник	Зовнішня підтримка окремих компонентів	Неконтрольований привілейований доступ	Іменні допуски, сеансовий доступ, запис дій, SLA інцидентів
Відновлення	Щоденні резервні копії	Недоступність або компрометація копій	Ізоляція, шифрування, регулярне тестове відновлення

Другий квартал присвячений цільовому профілю й базовим платформним контролям: IAM/PAM, сегментації, журналюванню, резервуванню, керуванню вразливостями, конфігураціями та ключами.

Паралельно формуються вимоги до ОІД, постачальників і персоналу. Кожний впроваджений контроль одразу отримує власника, параметр, тест і місце зберігання доказу.

Третій квартал переводить засоби в стабільні процеси. Проводяться тестові відновлення, навчання з інцидентів, перевірки технічних каналів, перегляд привілеїв, оцінювання постачальників і збір доказів за повний контрольний період. Пробний аудит виявляє розриви між документацією та практикою. Критичні недоліки усуваються до початку незалежного оцінювання.

Четвертий квартал охоплює фінальну внутрішню перевірку, незалежне оцінювання, коригувальні дії та авторизацію. Одночасно затверджується календар безперервного контролю на наступний рік. Проєктна команда не розпускається повністю: її функції переходять до постійних власників процесів, а координатор профілю контролює зміни, докази та підготовку до планової авторизації.

Таблиця 11. Річний план побудови системи безпеки ОІД

Реальний календар залежить від масштабу й вихідної зрілості. Для великої системи окремі потоки виконуються паралельно, але критичні залежності не можна переставляти: профіль не затверджується без сфери й ризиків; доказ не створюється без реалізації; оцінювання не починається з невідомими блокуючими недоліками; авторизація не завершує управління змінами. Ця послідовність зменшує переробки й робить результат відтворюваним.

Таблиця 10

Річний план побудови системи безпеки ОІД

Період	Фокус	Ключові результати	Критерій переходу
Місяці 1–3	Сфера, інформація, ОІД, ризики	Паспорт системи, потоки, модель загроз	Затверджені межі й пріоритети
Місяці 4–6	Цільовий профіль і базові контролі	IAM/PAM, журнали, резерви, ключі, сегментація	Кожна вимога має реалізацію й тест
Місяці 7–9	Операційна сталість і докази	Відновлення, навчання, постачальники, пробний аудит	Немає невідомих блокуючих недоліків
Місяці 10–12	Оцінювання й авторизація	Оцінювальний звіт, коригування, авторизаційний пакет	Запущений безперервний контроль

Необхідно відмітити, що практична система безпеки ОІД не може бути зведена до комплекту технічних засобів або разового авторизаційного пакета. Вона має одночасно охоплювати інформацію, системну архітектуру, контрольовану зону, персонал, постачальників, носії, резервування, журнали, інциденти та технічні канали витоку.

Ризик-орієнтована методика перетворює профіль на керований цикл: класифікація даних — визначення меж — аналіз ризиків — цільовий профіль — реалізація — докази — оцінювання — авторизація — безперервний контроль. Кількісні показники корисні лише разом із якісною оцінкою критичних невиконаних вимог і перевіркою доказів.

Перспективним напрямом є апробація методики на реальних системах різних класів, калібрування ваг показників за результатами незалежних оцінювань і розроблення засобів автоматизованого контролю актуальності доказів.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

1. У статті розроблено та подано ризик-орієнтовану методику побудови системи безпеки об’єкта інформаційної діяльності для роботи з інформацією з обмеженим доступом. Методика узгоджує системний контур кіберзахисту з фізичним та інженерно-технічним контуром об’єкта, охоплює класифікацію інформації, визначення меж довіри, аналіз ризиків, формування цільового профілю, реалізацію контролів, підготовку доказової бази, незалежне оцінювання, авторизацію та безперервний контроль.

2. Запропоновано аналітичні показники притаманного і залишкового ризику, зваженого покриття вимог, повноти доказів та інтегральної готовності. Показано, що кількісні оцінки мають застосовуватися разом із блокуючими критеріями та експертною перевіркою.

3. Практичне застосування продемонстровано на умовному сценарії обробки службової інформації; наведено матрицю відповідальності RACI та річну послідовність упровадження.

4. Наукова новизна полягає у формалізації наскрізного зв’язку «ризик — вимога — реалізація — доказ — рішення про авторизацію» для системного та фізичного контурів ОІД.

5. Результати придатні для планування впровадження, внутрішнього аудиту й підготовки до незалежного оцінювання. Запропоновані формули мають методичний, а не нормативний статус

Література

1. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20

2. Про затвердження порядків з питань розроблення та затвердження профілів безпеки і авторизації з безпеки інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем: постанова Кабінету Міністрів України від 18.06.2025 № 712. URL: https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF

3. Базовий профіль безпеки системи, в якій обробляється відкрита або конфіденційна інформація: наказ Адміністрації Держспецзв'язку від 30.06.2025 № 409. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=69624

4. Базовий профіль безпеки системи, в якій обробляється службова інформація: наказ Адміністрації Держспецзв'язку від 04.07.2025 № 419. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=72460

5. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

6. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17

7. Про затвердження Порядку ведення переліку авторизованих систем з безпеки: наказ Адміністрації Держспецзв'язку від 11.07.2025 № 434. URL: https://zakon.rada.gov.ua/laws/show/z1140-25

8. Про затвердження Вимог до суб'єктів оцінювання: наказ Адміністрації Держспецзв'язку від 11.07.2025 № 438. URL: https://zakon.rada.gov.ua/laws/show/z1125-25

9. Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 № 1229/99. URL: https://zakon.rada.gov.ua/laws/show/1229/99

10. Про затвердження Порядку оцінювання стану кіберзахисту: постанова Кабінету Міністрів України від 31.12.2025 № 1799. URL: https://zakon.rada.gov.ua/laws/show/1799-2025-%D0%BF

11. Про затвердження Порядку підтвердження постачальниками відповідності впроваджених заходів безпеки інформації: наказ Адміністрації Держспецзв'язку від 17.12.2025 № 836. URL: https://zakon.rada.gov.ua/laws/show/z1978-25

12. Про затвердження Вимог з кіберзахисту об'єктів критичної інфраструктури: наказ Адміністрації Держспецзв'язку від 07.10.2025 № 403. URL: https://zakon.rada.gov.ua/laws/show/z1599-25

13. Про внесення змін до постанови Кабінету Міністрів України від 18 червня 2025 р. № 712: постанова Кабінету Міністрів України від 10.04.2026 № 493. URL: https://zakon.rada.gov.ua/laws/show/493-2026-%D0%BF

14. Методичні рекомендації з формування цільового профілю безпеки інформації. Держспецзв'язку. URL: https://www.cip.gov.ua/ua/news/derzhspeczv-yazku-skhvalila-metodichni-rekomendaciyi-z-formuvannya-cilovogo-profilyu-bezpeki-informaciyi-nastupnii-krok-do-novoyi-modeli-deklaruvannya-vidpovidnosti-sistem-zakhistu

References

1. Verkhovna Rada of Ukraine. (2025). Law of Ukraine No. 4336-IX on amendments concerning information protection and cybersecurity. https://zakon.rada.gov.ua/laws/show/4336-20 [in Ukrainian].

2. Cabinet of Ministers of Ukraine. (2025). Resolution No. 712 on procedures for developing security profiles and security authorization. https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF [in Ukrainian].

3. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Baseline security profile for systems processing open or confidential information (Order No. 409). https://cip.gov.ua/services/cm/api/attachment/download?id=69624 [in Ukrainian].

4. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Baseline security profile for systems processing official information (Order No. 419). https://cip.gov.ua/services/cm/api/attachment/download?id=72460 [in Ukrainian].

5. Verkhovna Rada of Ukraine. (1994). Law of Ukraine No. 80/94-VR on information protection in information and communication systems. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 [in Ukrainian].

6. Verkhovna Rada of Ukraine. (2011). Law of Ukraine No. 2939-VI on access to public information. https://zakon.rada.gov.ua/laws/show/2939-17 [in Ukrainian].

7. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Procedure for maintaining the list of security-authorized systems (Order No. 434). https://zakon.rada.gov.ua/laws/show/z1140-25 [in Ukrainian].

8. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Requirements for assessment entities (Order No. 438). https://zakon.rada.gov.ua/laws/show/z1125-25 [in Ukrainian].

9. President of Ukraine. (1999). Regulation on technical protection of information in Ukraine (Decree No. 1229/99). https://zakon.rada.gov.ua/laws/show/1229/99 [in Ukrainian].

10. Cabinet of Ministers of Ukraine. (2025). Procedure for assessing the state of cybersecurity (Resolution No. 1799). https://zakon.rada.gov.ua/laws/show/1799-2025-%D0%BF [in Ukrainian].

11. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Procedure for suppliers to confirm compliance of implemented information-security measures (Order No. 836). https://zakon.rada.gov.ua/laws/show/z1978-25 [in Ukrainian].

12. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Cybersecurity requirements for critical infrastructure facilities (Order No. 403). https://zakon.rada.gov.ua/laws/show/z1599-25 [in Ukrainian].

13. Cabinet of Ministers of Ukraine. (2026). Resolution No. 493 amending Resolution No. 712. https://zakon.rada.gov.ua/laws/show/493-2026-%D0%BF [in Ukrainian].

14. State Service of Special Communications and Information Protection of Ukraine. (2025). Methodological recommendations for developing a target information-security profile. https://www.cip.gov.ua/ua/news/derzhspeczv-yazku-skhvalila-metodichni-rekomendaciyi-z-formuvannya-cilovogo-profilyu-bezpeki-informaciyi-nastupnii-krok-do-novoyi-modeli-deklaruvannya-vidpovidnosti-sistem-zakhistu [in Ukrainian].