УДК 004.056.5:[351.751.5:004.77 DOI: 10.31673/2409-7292.2026.034811

Рижаков Микола Миколайович
доктор філософії, старший викладач кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0006-3377-7061
E-mail: nykolay.ryjakov@gmail.com

Котенко Андрій Миколайович
кандидат технічних наук, доцент, доцент кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-0483-6353
E-mail: dutkotenko@gmail.com

Іванченко Ігор Сергійович
кандидат технічних наук, доцент, професор кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-3415-9039
E-mail: igor-p-l@ukr.net

Пепа Юрій Володимирович
кандидат технічних наук, доцент, професор кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-2073-1364
E-mail: yurka14@gmail.com

Щербак Тетяна Леонідівна
Доцент кафедри технічного захисту інформації
Державний університет «Київський Авіаційний інститут», Київ, Україна
ORCID: 0000-0003-1170-8154
E-mail: tetiana.shcherbak@npp.kai.edu.ua

МЕТОДИКА ФОРМУВАННЯ ПРОФІЛЮ БЕЗПЕКИ ТА АВТОРИЗАЦІЇ СИСТЕМ, У ЯКИХ ОБРОБЛЯЄТЬСЯ ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ

У статті розроблено методичний підхід до формування профілю безпеки та авторизації інформаційних, електронних комунікаційних, інформаційно-комунікаційних і технологічних систем, у яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом. Обґрунтовано перехід від разового проєктного підтвердження відповідності до ризик-орієнтованої профільної моделі, що передбачає безперервне управління вимогами, доказами, ризиками та змінами. Розкрито співвідношення базового, галузевого та цільового профілів, роль власника або розпорядника системи, порядок оцінювання дотримання цільового профілю та види авторизації. Запропоновано послідовність визначення правового режиму інформації, встановлення меж системи, декомпозиції вимог до перевірюваних результатів, формування доказової бази, оцінювання відповідності та підтримання профілю впродовж життєвого циклу. Для внутрішнього контролю запропоновано систему індикаторів підтвердженості застосовності, покриття вимог, повноти доказів та авторизаційної готовності. Практична цінність підходу полягає у забезпеченні простежуваності між нормативними вимогами, заходами захисту та фактичними доказами їх реалізації. Методи дослідження охоплюють нормативно-правовий і порівняльний аналіз, структурно-функціональне моделювання, декомпозицію вимог та аналіз життєвого циклу. Сформовано практичну дорожню карту переходу до профільної моделі, що поєднує інвентаризацію систем, аналіз ризиків, розроблення цільового профілю, перевірку критичних вимог і підготовку авторизаційного пакета. Підхід може бути використаний для планування переходу, виявлення критичних розривів та контролю готовності системи.

Ключові слова: інформація з обмеженим доступом, профіль безпеки, цільовий профіль, авторизація системи, оцінювання відповідності, кіберзахист, ризик-орієнтований підхід.

Вступ та формулювання проблеми

У сучасних умовах цифровізації державного управління, розвитку електронних сервісів, хмарних технологій та інформаційно-комунікаційних систем особливої актуальності набуває питання побудови формалізованої, перевірюваної та життєздатної системи захисту

інформації. Для систем, у яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, недостатньо лише розробити комплект документації чи впровадити окремі технічні засоби захисту. Необхідно забезпечити доведення того, що обрані організаційні, технічні, криптографічні та фізичні заходи відповідають реальним ризикам, фактичній архітектурі системи, правовому режиму інформації та умовам її експлуатації [1-3].

Особливого значення це питання набуло після оновлення нормативної бази у сфері кіберзахисту державних інформаційних ресурсів та інформації з обмеженим доступом. Нова модель передбачає перехід від логіки одноразового створення комплексної системи захисту інформації з подальшим отриманням атестата відповідності до профільної моделі, у межах якої безпека розглядається як безперервна функція управління. Такий підхід передбачає визначення сфери системи, вибір базового або галузевого профілю, розроблення цільового профілю, оцінювання його дотримання та прийняття авторизаційного рішення [1-3, 8-13].

У нормативно-правовому контексті важливо розмежовувати поняття інформації з обмеженим доступом та об’єкта інформаційної діяльності. Інформація з обмеженим доступом охоплює конфіденційну, службову та таємну інформацію, порядок доступу до якої визначається законом або уповноваженим власником. Об’єкт інформаційної діяльності є простором, приміщенням, інженерно-технічною спорудою або комплексом, де здійснюється діяльність, пов’язана з інформацією, що підлягає захисту. Тому профілі безпеки й авторизація систем стосуються передусім інформаційних, електронних комунікаційних, інформаційно-комунікаційних і технологічних систем, тоді як захист об’єктів інформаційної діяльності включає також фізичний, інженерний та технічний контур: контрольовані зони, акустичні та віброакустичні канали, побічні електромагнітні випромінювання, несанкціоновані пристрої та інші канали витоку [2, 5-7].

Актуальність теми визначається тим, що власник або розпорядник системи повинен не лише формально виконати нормативні вимоги, а й довести здатність системи підтримувати прийнятний рівень ризику протягом усього життєвого циклу. Це потребує методики, яка поєднує нормативно-правовий аналіз, ризик-орієнтоване управління, технічну реалізацію заходів захисту та доказову базу для оцінювання й авторизації.

Аналіз останніх досліджень і публікацій

Питання захисту інформації в інформаційно-комунікаційних системах традиційно розглядається в контексті побудови комплексних систем захисту інформації, застосування організаційно-технічних заходів, контролю доступу, криптографічного та технічного захисту інформації. У наукових та нормативно-методичних джерелах значна увага приділяється визначенню вимог до захисту інформації, побудові моделей загроз, оцінюванню ризиків, підтвердженню відповідності та експлуатаційному супроводу систем захисту [2, 4, 6, 7].

Водночас зміна нормативного середовища актуалізує потребу в переосмисленні попередніх підходів. Якщо раніше акцент часто робився на розробленні проєктної документації, проведенні державної експертизи та отриманні підтверджувального документа, то профільна модель зміщує фокус на постійне управління вимогами, доказами й ризиками. У такій моделі головним результатом стає не сам факт наявності документації, а здатність організації у будь-який момент підтвердити, що кожна релевантна вимога профілю реалізована, перевірена, має власника, параметр контролю та актуальний доказ [1, 3, 8-13].

Аналіз сучасних підходів до оцінювання кіберзахисту свідчить, що ключовими стають принципи простежуваності, доказовості, ризик-орієнтованості та безперервного контролю. Простежуваність означає наявність зв’язку між законом, базовим профілем, цільовим профілем, конкретним заходом захисту, технічною конфігурацією та доказом виконання. Доказовість передбачає, що підтвердженням є не лише політика або наказ, а й операційні журнали, результати тестів, конфігураційні звіти, акти перевірок, протоколи навчань, документи управління змінами та інші матеріали, які підтверджують фактичну роботу контролю. Ризик-орієнтованість дозволяє адаптувати параметри контролів до критичності

системи, однак не повинна використовуватися як підстава для ігнорування мінімальних обов'язкових вимог [14-20].

Недостатньо дослідженим залишається питання побудови цілісної методики, яка дозволяє власнику або розпоряднику системи перейти від загальних нормативних вимог до практично керованого цільового профілю, організувати доказову базу, провести оцінювання та забезпечити підтримання відповідності після авторизації. Саме це визначає науково-практичну значущість статті.

Мета статті та завдання дослідження

Метою статті є розроблення методичного підходу до побудови сучасного профілю безпеки та авторизації систем, у яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, з урахуванням ризик-орієнтованої профільної моделі управління захистом.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Визначити сферу застосування профільної моделі безпеки для систем, у яких обробляється інформація з обмеженим доступом.

2. Розкрити співвідношення базового, галузевого та цільового профілів безпеки.

3. Визначити послідовність формування цільового профілю безпеки та його доказової бази.

4. Обґрунтувати роль власника або розпорядника системи у прийнятті залишкового ризику та забезпеченні авторизації.

5. Запропонувати практичну дорожню карту переходу до профільної моделі безпеки.

Методи дослідження включають нормативно-правовий аналіз, структурно-функціональне моделювання, порівняльний аналіз профілів безпеки, декомпозицію вимог до перевірюваних результатів, аналіз життєвого циклу системи та методи ризик-орієнтованого управління.

Виклад основного матеріалу дослідження

1. Нормативна архітектура сучасної профільної моделі безпеки [1-3, 8-13]

Сучасна модель захисту систем, у яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вибудовується як ієрархія взаємопов'язаних управлінських і технічних рішень. Закон визначає загальний обов'язок забезпечити захист інформації в авторизованих системах або застосувати інший передбачений законом механізм підтвердження відповідності. Підзаконні акти деталізують порядок розроблення профілів, процедури оцінювання та авторизації. Базові й галузеві профілі перетворюють загальний обов'язок на набір перевірюваних вимог. Цільовий профіль конкретизує ці вимоги для реальної системи, її архітектури, функцій, ризиків і режиму експлуатації. На практиці ця конструкція не повинна сприйматися як сукупність відокремлених документів. Рішення про сферу застосування визначає вид базового профілю; результати аналізу ризиків уточнюють параметри цільового профілю; реалізація кожної вимоги породжує доказ; сукупність доказів формує пакет для незалежного оцінювання; результати оцінювання стають підставою для авторизаційного рішення. Якщо між цими елементами немає простежуваного зв'язку, навіть значний обсяг документації не доводить фактичну керованість захисту.

Першим аналітичним етапом є визначення сфери застосування. Необхідно встановити правовий статус власника або розпорядника системи, вид інформації, що обробляється, наявність державних інформаційних ресурсів або інформації з обмеженим доступом, функціональне призначення системи, критичність процесів, зовнішні залежності, інтеграції, використання хмарних сервісів і статус об'єктів критичної інформаційної інфраструктури. Один і той самий програмний продукт може підпадати під різні правові режими залежно від того, хто ним володіє, які дані обробляються та які функції він підтримує [1-7].

Сфера системи повинна включати не лише сервери й робочі станції, а й засоби адміністрування, мережеві сегменти, журнали подій, резервні копії, сховища ключів, віддалені майданчики, інтеграційні шлюзи, робочі місця адміністраторів, технічні засоби об'єктів

© Рижаков М.М., Котенко А.М., Іванченко І.С., Пепа Ю.В., Щербак Т.Л. Методика формування профілю безпеки та авторизації систем, у яких обробляється інформація з обмеженим доступом. Сучасний захист інформації, 3(67), 119–127. https://doi.org/10.31673/2409-7292.2026.034811

інформаційної діяльності та канали підтримки. Виключення будь-якого компонента зі сфери оцінювання допускається лише тоді, коли доведено, що він не обробляє захищувану інформацію і не може впливати на безпеку системи через довірчі зв'язки.

Результатом цього етапу має бути паспорт сфери, який містить опис послуг і функцій, реєстр інформації, схему компонентів, карту потоків даних, перелік зовнішніх залежностей, відповідальних осіб, застосовні профілі та спеціальні нормативні вимоги.

Таблиця 1

Критерії визначення застосовності профільної моделі

Критерій	Контрольне питання	Типовий доказ	Управлінський результат
Статус власника	Чи є власник або розпорядник державним органом, державною установою або органом місцевого самоврядування?	Статут, положення, розпорядчий акт	Визначення прямих нормативних обов'язків
Вид інформації	Чи обробляються державні інформаційні ресурси або ІзОД?	Реєстр даних, перелік відомостей	Вибір базового профілю
Функціональне призначення	Які державні або критичні функції підтримує система?	Каталог послуг, BIA, паспорт системи	Визначення критичності
Межі та інтеграції	Які компоненти, канали й сервіси впливають на безпеку?	Архітектурна схема, карта потоків	Фіксація повної сфери оцінювання
Спеціальне регулювання	Чи діють спеціальні вимоги для державної таємниці, фінансового сектору або критичної інфраструктури?	Юридичний висновок	Додавання спеціальних контролів

2. Базовий, галузевий і цільовий профілі безпеки

Профільна модель передбачає кілька рівнів деталізації вимог. Базовий профіль визначає мінімальний набір вимог залежно від виду інформації або функціонального призначення системи. Галузевий профіль уточнює базові вимоги з урахуванням специфіки певної сфери, галузевих ризиків, стандартів і політик. Цільовий профіль формується власником або розпорядником конкретної системи та перетворює загальні вимоги на конкретні заходи, налаштування, ролі, процедури й докази.

Цільовий профіль не може бути формальною копією базового. Він має враховувати архітектуру системи, її межі, зовнішні з'єднання, ролі користувачів і адміністраторів, місця обробки інформації з обмеженим доступом, застосовні хмарні сервіси, модель загроз, результати аналізу ризиків, вимоги технічного та криптографічного захисту, а також галузеві вимоги, якщо вони існують.

Базові профілі зазвичай охоплюють такі напрями: управління доступом, ідентифікація та автентифікація, аудит і моніторинг, конфігураційне управління, управління вразливостями, реагування на інциденти, резервне копіювання та відновлення, захист носіїв, фізична безпека, управління персоналом і постачальниками. Для службової інформації вимоги можуть бути суворішими, зокрема щодо контролю носіїв, резервних копій, криптографічного захисту, зовнішніх послуг і ризиків ланцюга постачання. [8–13]

Під час формування цільового профілю кожна вимога повинна бути декомпонована до перевірюваного результату. Наприклад, вимога щодо управління обліковими записами не може оцінюватися одним формальним пунктом. Вона має охоплювати створення, погодження, зміну, блокування, видалення, періодичний перегляд, привілейовані та сервісні облікові записи, тимчасовий доступ і моніторинг аномалій.

Ризик-орієнтований підхід дозволяє деталізувати параметри, але не скасовує мінімальні обов'язкові вимоги. Організація може посилювати контролі для критичних систем, обґрунтовувати компенсуючі заходи, визначати пріоритети впровадження, але не повинна замінювати нормативну вимогу суб'єктивним рішенням про низький ризик. Якщо технічна

© Рижаков М.М., Котенко А.М., Іванченко І.С., Пепа Ю.В., Щербак Т.Л. Методика формування профілю безпеки та авторизації систем, у яких обробляється інформація з обмеженим доступом. Сучасний захист інформації, 3(67), 119–127. https://doi.org/10.31673/2409-7292.2026.034811

платформа не підтримує необхідний механізм, це повинно бути зафіксовано як обмеження із зазначенням тимчасового контролю, строку модернізації, відповідального керівника та залишкового ризику.

Таблиця 2

Паспорт вимоги цільового профілю

Поле	Зміст	Контрольне питання
Ідентифікатор	Стабільний код вимоги та версії	Чи можна простежити історію зміни?
Походження	Базовий профіль, галузевий профіль, закон, ризик	Чому вимога є обов'язковою?
Мета безпеки	Очікуваний захисний результат	Який сценарій загрози має бути запобігнутий або виявлений?
Параметр	Частота, строк, охоплення, поріг	Що саме можна перевірити?
Реалізація	Технічний або організаційний механізм	Де і ким виконується контроль?
Доказ	Журнал, протокол, конфігурація, тест	Чи є доказ актуальним і відтворюваним?
Власник	Відповідальна роль	Хто усуває відхилення?

3. Доказовість, оцінювання та авторизація системи

Однією з ключових ознак сучасної профільної моделі є доказовість. Докази повинні проєктуватися одночасно із контролями. Якщо журнал зберігається коротший період, ніж охоплює перевірка, організація не зможе підтвердити роботу контролю. Якщо звіт формується вручну без фіксації джерела даних, його неможливо відтворити. Тому для кожної вимоги мають бути визначені формат доказу, джерело, строк зберігання, контроль цілісності, доступ до доказу, відповідальна особа та процедура внутрішньої перевірки.

Якість доказу доцільно оцінювати за п'ятьма критеріями: належність, повнота, актуальність, цілісність і відтворюваність. Належність означає, що доказ прямо підтверджує конкретну вимогу. Повнота означає охоплення всіх релевантних компонентів, ролей і періодів. Актуальність підтверджує, що доказ відповідає поточній версії системи. Цілісність гарантує, що доказ не був змінений безконтрольно. Відтворюваність означає, що інша компетентна особа може повторити перевірку та отримати зіставний результат.

Оцінювання дотримання цільового профілю має включати аналіз документів, технічних конфігурацій, журналів, результатів тестів, процесів реагування на інциденти, процедур управління змінами та доказів фактичної експлуатації контролів. Оцінювач не повинен створювати доказ замість організації або підмінювати власника вимоги. Його завдання – перевірити, чи відповідають реалізовані заходи затвердженому цільовому профілю та чи підтверджені вони належними доказами [3, 12, 13].

Авторизація системи може бути первинною, плановою або позаплановою. Первинна авторизація проводиться до початку експлуатації системи. Планова авторизація здійснюється після попередньої авторизації на основі щорічного перегляду ризиків, актуалізації профілю та повторного оцінювання. Позапланова авторизація необхідна у разі суттєвих змін: оновлення базового або галузевого профілю, зміни архітектури, перенесення системи до хмари, підключення зовнішнього сервісу, інциденту з компрометацією, зміни правового режиму інформації або критичного постачальника [3, 10-13].

Особливе місце в авторизаційній моделі займає відповідальність власника або розпорядника системи. Створення підрозділу з кіберзахисту або залучення незалежного оцінювача не означає передачі їм управлінської відповідальності за прийняття залишкового ризику. Керівник затверджує межі системи, ресурси, пріоритети, допустимий ризик і цільовий профіль. Підрозділи кіберзахисту, ІТ, режимний і юридичний напрями забезпечують реалізацію, але остаточне рішення про прийнятність залишкового ризику має залишатися на рівні власника або уповноваженого керівництва.

© Рижаков М.М., Котенко А.М., Іванченко І.С., Пепа Ю.В., Щербак Т.Л. Методика формування профілю безпеки та авторизації систем, у яких обробляється інформація з обмеженим доступом. Сучасний захист інформації, 3(67), 119–127. https://doi.org/10.31673/2409-7292.2026.034811

Таблиця 3

Види авторизації та управлінські тригери

Вид авторизації	Коли проводиться	Основний пакет	Управлінський тригер
Первинна	До початку експлуатації	Цільовий профіль, результати оцінювання, авторизаційний лист	Введення системи в експлуатацію
Планова	Після попередньої авторизації	Оновлений аналіз ризиків, докази, повторне оцінювання	Щорічний цикл контролю
Позапланова	Після суттєвих змін	Актуалізований профіль, аналіз змін, оцінювання релевантних вимог	Зміна профілю, архітектури, постачальника або режиму даних

4. Управління життєвим циклом, змінами та постачальниками

Після авторизації система не повинна випадати з контуру управління безпекою. Планова авторизація має спиратися не на повторне використання старого пакета документів, а на актуальний аналіз ризиків і підтвердження безперервної роботи контролів. Щорічний перегляд повинен охоплювати зміни архітектури, програмного забезпечення, зовнішніх сервісів, складу даних, об’єктів інформаційної діяльності, персоналу, постачальників, загроз та інцидентів.

Календарний перегляд не замінює подієвого. Суттєва зміна може виникнути одразу після планової авторизації. До таких змін належать перенесення системи в хмару, новий канал віддаленого доступу, приєднання зовнішньої системи, зміна контрольованої зони, інцидент з компрометацією, зміна критичного постачальника або оновлення базового профілю. Для кожної такої зміни необхідно оформлювати короткий пакет впливу: опис зміни, компоненти й дані, ризики, вимоги профілю, необхідні тести, оновлення доказів, відповідальні особи та рішення щодо потреби в позаплановій авторизації.

Передача функції постачальнику не означає передачу йому відповідальності власника системи. Договір із постачальником має визначати види інформації, дозволені місця обробки, ролі адміністраторів, вимоги до субпідрядників, строки повідомлення про інциденти, журналювання, резервування, повернення і знищення даних, право на аудит та обов’язок надання доказів. Якщо ці положення не відображені в договорі, організація може опинитися в ситуації, коли вимога цільового профілю формально існує, але юридично не може бути перевірена.

Для хмарних сервісів важливо фіксувати матрицю спільної відповідальності. Постачальник може відповідати за фізичну інфраструктуру або платформу, але замовник залишається відповідальним за налаштування ідентичностей, ключі, журнали, дані, резервні копії та реагування. Тому формулювання про «сертифіковану хмару» саме по собі не доводить безпеку конкретного середовища. Потрібні конфігураційні докази, журнали, тести відновлення, контроль привілейованого доступу та план виходу з хмарного сервісу [14-17].

5. Аналітична модель нормативної готовності

Для внутрішнього управління великою кількістю вимог доцільно використовувати аналітичну модель нормативної готовності. Така модель не замінює нормативного оцінювання або авторизації, але допомагає порівнювати стан різних систем, визначати критичні розриви та планувати ресурси [18-20].

Індекс підтвердженості застосовності може бути поданий у вигляді:

$$Z = \frac{\sum_k \; w_k \cdot a_k}{\sum_k \; w_k}, \qquad (1)$$

де a_k – оцінка підтвердженості критерію застосовності; w_k – вага критерію застосовності.

Зважене покриття вимог цільового профілю може визначатися так:

$$C_t = \frac{\sum_j \quad v_j \cdot x_j}{\sum_j \quad v_j}, \tag{2}$$

де x_j – ступінь виконання вимоги профілю; v_j — критичність вимоги.

Повнота верифікованої доказової бази може визначатися як:

$$D_e = \frac{N_{\text{verified}}}{N_{\text{required}}} \cdot 100\%, \tag{3}$$

де Nrequired – кількість обов'язкових доказів за актуальною версією профілю; Nverified – кількість доказів, що пройшли перевірку належності, повноти, актуальності, цілісності та відтворюваності.

Ілюстративний індекс авторизаційної готовності може бути поданий так:

$$A_r = \beta_1 C_t + \beta_2 D_e + \beta_3 G + \beta_4 O, \tag{4}$$

де C_t – покриття профілю; D_e – повнота доказів; G – зрілість управління ризиками та змінами; O – операційна сталість контролів; β_1–β_4 – вагові коефіцієнти, які затверджуються організацією.

Водночас така модель повинна застосовуватися лише після перевірки блокуючих критеріїв: правильно визначеної сфери, наявності релевантного базового профілю, відсутності критичних невиконаних вимог, прийнятності залишкового ризику та достовірності доказів. Високий середній індекс не може компенсувати критичну невідповідність.

Результати дослідження та практичні рекомендації

Практичний перехід до профільної моделі доцільно організувати у кілька часових горизонтів.

На етапі 0-30 днів здійснюється управлінський запуск: призначення відповідальних осіб, формування міжфункціональної групи, інвентаризація систем, визначення правового режиму інформації та попередня перевірка застосовності. Ключовий результат – затверджений перелік систем, власників, категорій даних і строків переходу.

На етапі 31-90 днів формуються межі пріоритетних систем, архітектурні схеми, карти потоків даних, перелік зовнішніх сервісів, базовий або галузевий профіль і реєстр вимог. Паралельно проводиться аналіз ризиків та інвентаризація наявних контролів.

На етапі 91-180 днів розробляється та затверджується цільовий профіль, реалізуються пріоритетні технічні, організаційні, криптографічні та фізичні заходи, оновлюються договори з постачальниками, запускається репозиторій доказів і календар безперервного контролю.

На етапі 181-270 днів проводяться випробування, пробний аудит, перевірка критичних вимог і коригування параметрів, які неможливо стабільно вимірювати.

На етапі 271-365 днів завершується повний цикл: внутрішня перевірка, усунення блокуючих недоліків, незалежне оцінювання, прийняття авторизаційного рішення, внесення відомостей до відповідного переліку та запуск планового перегляду.

Остаточним критерієм переходу є не кількість створених документів, а здатність організації у будь-який момент відповісти на п'ять питань: що саме захищається; на якій правовій підставі; які ризики прийняті; як реалізована кожна критична вимога; яким актуальним доказом підтверджується її робота.

Висновки та перспективи подальших досліджень

1. У статті запропоновано методичний підхід до побудови сучасного профілю безпеки та авторизації систем, у яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом. Обґрунтовано, що профільна модель змінює управлінську логіку захисту: від разового підтвердження відповідності до безперервного управління ризиками, вимогами, доказами та змінами.

© Рижаков М.М., Котенко А.М., Іванченко І.С., Пепа Ю.В., Щербак Т.Л. Методика формування профілю безпеки та авторизації систем, у яких обробляється інформація з обмеженим доступом. Сучасний захист інформації, 3(67), 119–127. https://doi.org/10.31673/2409-7292.2026.034811

2. Показано, що нормативно коректний проєкт починається не з вибору засобів захисту, а з визначення сфери системи, правового режиму інформації, меж відповідальності, застосовного базового або галузевого профілю. Цільовий профіль повинен конкретизувати мінімальні вимоги для реальної архітектури, визначати параметри контролів, власників, строки, докази та механізми підтримання відповідності.

3. Встановлено, що доказова база є центральним елементом авторизаційної готовності. Документація, технічні конфігурації, журнали, протоколи, результати тестів і акти перевірок повинні бути належними, повними, актуальними, цілісними та відтворюваними. Лише за таких умов оцінювання дотримання цільового профілю може підтвердити фактичний стан захищеності системи.

4. Запропоновано аналітичну модель нормативної готовності, яка може застосовуватися як внутрішній інструмент планування та контролю, але не замінює незалежного оцінювання або авторизаційного рішення. Перспективним напрямом подальших досліджень є розроблення автоматизованих засобів ведення реєстру вимог цільового профілю, управління доказами, оцінювання змін і формування авторизаційного пакета для систем різного рівня критичності.

Перелік посилань

1. Закон України «Про внесення змін до деяких законів України щодо удосконалення правових засад забезпечення кіберзахисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» від 27.03.2025 № 4336-IX. https://zakon.rada.gov.ua/laws/show/4336-20#Text.

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

3. Постанова Кабінету Міністрів України «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних і технологічних систем» від 18.06.2025 № 712. https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text.

4. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. https://zakon.rada.gov.ua/laws/show/2163-19#Text.

5. Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI. https://zakon.rada.gov.ua/laws/show/2939-17#Text.

6. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 № 3475-IV. https://zakon.rada.gov.ua/laws/show/3475-15#Text.

7. Указ Президента України «Про Положення про технічний захист інформації в Україні» від 27.09.1999 № 1229/99. https://zakon.rada.gov.ua/laws/show/1229/99#Text.

8. Базовий профіль безпеки системи, де обробляється відкрита або конфіденційна інформація: наказ Адміністрації Держспецзв'язку від 30.06.2025 № 409.

9. Базовий профіль безпеки системи, де обробляється службова інформація: наказ Адміністрації Держспецзв'язку від 02.07.2025 № 419.

10. Порядок ведення переліку авторизованих систем з безпеки: наказ Адміністрації Держспецзв'язку від 11.07.2025 № 434.

11. Вимоги до суб'єктів оцінювання: наказ Адміністрації Держспецзв'язку від 11.07.2025 № 438.

12. Постанова Кабінету Міністрів України «Про внесення змін до постанов Кабінету Міністрів України від 18 червня 2025 р. № 712 і від 31 грудня 2025 р. № 1799» від 10.04.2026 № 493. https://zakon.rada. gov.ua /laws/show/493-2026-%D0%BF#Text.

13. Постанова Кабінету Міністрів України «Про затвердження Порядку оцінювання стану кіберзахисту» від 31.12.2025 № 1799. https://zakon.rada.gov.ua/laws/show/1799-2025-%D0%BF#Text.

14. Порядок підтвердження постачальниками відповідності впроваджених заходів безпеки інформації: наказ Адміністрації Держспецзв'язку від 17.12.2025 № 836.

15. Вимоги з кіберзахисту об'єктів критичної інфраструктури: наказ уповноваженого органу від 07.10.2025 № 403.

16. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001.

17. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. https://www.iso.org/standard/75652.html.

18. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. https://www.iso.org/standard/80585.html.

19. NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29.

20. NIST. (2020). Security and Privacy Controls for Information Systems and Organizations (Special Publication 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5.

Mykola Ryzhakov
PhD, Senior Lecturer, Department of Technical Systems of Cybersecurity
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0006-3377-7061
E-mail: nykolay.ryjakov@gmail.com

Andrii Kotenko
Candidate of Technical Sciences, Associate Professor, Department of Technical Systems of Cybersecurity
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-0483-6353
E-mail: dutkotenko@gmail.com

Ihor Ivanchenko
Candidate of Technical Sciences, Associate Professor, Professor, Department of Technical Systems of Cybersecurity
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-3415-9039
E-mail: igor-p-l@ukr.net

Yurii Pepa
Candidate of Technical Sciences, Associate Professor, Professor, Department of Technical Systems of Cybersecurity
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-2073-1364
E-mail: yurka14@gmail.com

Tetiana Shcherbak
Associate Professor of the Department of Technical Information Protection
State University “Kyiv Aviation Institute”, Kyiv, Ukraine
ORCID: 0000-0003-1170-8154
E-mail: tetiana.shcherbak@npp.kai.edu.ua

METHODOLOGY FOR DEVELOPING A SECURITY PROFILE AND AUTHORIZING SYSTEMS THAT PROCESS RESTRICTED INFORMATION

The article develops a methodological approach to creating a security profile and authorizing systems that process state information resources or restricted information. The transition from one-time project-based conformity confirmation to a risk-oriented profile model requiring continuous management of requirements, evidence, risks, and changes is substantiated. The relationships among baseline, sectoral, and target security profiles are clarified, together with the responsibilities of the system owner or administrator, the procedure for assessing compliance with the target profile, and the types of authorization. The proposed sequence covers determination of the legal regime of information, definition of system boundaries, decomposition of requirements into verifiable outcomes, development of an evidence base, conformity assessment, and maintenance of the profile throughout the system life cycle. A set of internal indicators is introduced to characterize confirmation of applicability, weighted coverage of requirements, completeness of verified evidence, and authorization readiness. Particular attention is paid to management responsibility, supplier governance, cloud services, architectural changes, and transition from legacy comprehensive information protection projects. The practical value of the approach lies in establishing traceability between regulatory requirements, implemented security measures, responsible roles, control parameters, and current evidence of effective operation. The methodology may be used to plan the transition to the profile model, identify blocking gaps, and prepare an authorization package without replacing independent assessment or the authorization decision.

Keywords: restricted information, security profile, target profile, system authorization, conformity assessment, cybersecurity, risk-oriented approach.

Надійшла до редакції (Received): 03.08.2026
Прийнята до друку (Accepted): 08.09.2026
Опубліковано онлайн (Available online): 15.09.2026

© Рижаков М.М., Котенко А.М., Іванченко І.С., Пепа Ю.В., Щербак Т.Л. Методика формування профілю безпеки та авторизації систем, у яких обробляється інформація з обмеженим доступом. Сучасний захист інформації, 3(67), 119–127. https://doi.org/10.31673/2409-7292.2026.034811