МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ЕТИЧНІ, ПРАВОВІ ТА ТЕХНІЧНІ АСПЕКТИ РОЗРОБКИ ПОЛІТИК КІБЕРБЕЗПЕКИ В ОРГАНІЗАЦІЯХ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Єгор ДОНЦОВ

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Єгор ДОНЦОВ

Керівник: Юрій ЩАВІНСЬКИЙ
к.т.н., доцент

Рецензент:
к.т.н., доцент Юрій ПЕПА

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Донцову Єгору Андрійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Етичні, правові та технічні аспекти розробки політик кібербезпеки в організаціях"
керівник кваліфікаційної роботи Юрій ЩАВІНСЬКИЙ, к. техн. наук, доцент
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. № 467.
2. Строк подання кваліфікаційної роботи "11" грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: нормативні документи та стандарти інформаційної безпеки, кодекси професійної етики у сфері IT, інструкції та чинні політики кібербезпеки (знеособлені), статистика кіберінцидентів, технічні характеристики систем.
4. Перелік питань, які потрібно розробити:
   1. Проаналізувати нормативно-правову базу України та міжнародні стандарти у сфері розробки політик.
   2. Визначити ключові етичні аспекти та проблеми балансу між безпекою організації та правами користувачів.
   3. Провести аналіз практичних кейсів порушень безпеки, спричинених неефективними політиками.
   4. Дослідити існуючі методи оцінки ефективності політик.
   5. Розробити методику розробки та впровадження політик, що враховує етичні, правові та технічні вимоги.
   6. Сформулювати рекомендації щодо інтеграції технічних методів захисту в політики та розробити приклад політики.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Дослідження теоретичних основ та класифікації політик кібербезпеки. Аналіз нормативно-правової бази та етичних аспектів.	27.10.2025	
4.	Аналіз стану кібербезпеки на основі міжнародних звітів та дослідження кейсів порушень. Виявлення проблем інтеграції.	10.11.2025	
5.	Розробка методики розробки і впровадження політик. Створення пілотного проєкту та його технічна реалізація засобами SIEM-систем IBM QRadar.	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Єгор ДОНЦОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Донцов Є.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Етичні, правові та технічні аспекти розробки політик кібербезпеки в організаціях"
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Виконане здобувачем Донцовим Єгором дослідження має теоретичну повноту й практичну спрямованість, робота структурована логічно, містить аналіз нормативно-правової бази, огляд міжнародних стандартів, розгляд етичних дилем та приклади практичних кейсів. Робота містить раціональний аналіз етичних дилем (приватність та безпека, моніторинг працівників, прозорість політик), обґрунтовано підхід до оцінки ризиків з урахуванням прав людини та професійної етики.

ДОНЦОВ Єгор продемонстрував високий рівень теоретичної підготовки, володіння сучасними методами наукового аналізу та практичними навичками застосування засобів кіберзахисту.
Все це дозволяє оцінити кваліфікаційну роботу здобувача ДОНЦОВА Єгора на оцінку «відмінно» та рекомендувати присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою "Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Донцов Є.А. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувачу вищої освіти Донцову Єгору Андрійовичу
на тему “ Етичні, правові та технічні аспекти розробки політик кібербезпеки в організаціях ”

Актуальність. В умовах зростання кількості кіберінцидентів питання формування ефективних політик кібербезпеки набуває особливої актуальності. Сучасні організації стикаються не лише з технічними загрозами, а й із необхідністю дотримання правових вимог та етичних принципів, пов’язаних із захистом персональних даних, приватності користувачів і відповідальністю за обробку інформації. Водночас виникає потреба у забезпеченні балансу між впровадженням жорстких технічних заходів захисту та дотриманням етичних норм і прав користувачів, що залишається недостатньо дослідженим у наукових працях. У зв’язку з цим дослідження етичних, правових і технічних аспектів розробки політик кібербезпеки є актуальним і своєчасним, оскільки спрямоване на підвищення ефективності систем управління інформаційною безпекою організацій та формування науково обґрунтованих рекомендацій щодо розробки й впровадження політик, адаптованих до сучасних кіберзагроз і суспільних викликів.

Позитивні сторони

Робота поєднує міждисциплінарний підхід – етичний, юридичний і технічний – у єдиній методиці розробки політик, що є цінним практичним результатом для організацій, які прагнуть збалансувати безпеку й права користувачів. Практична значущість підтверджується наявністю конкретних рекомендацій та прикладів шаблонів політик, які можуть бути використані у практиці адміністрації інформаційної безпеки та SOC.

Матеріал викладено чітко, структура роботи логічна: вступ, огляд літератури та нормативно-правової бази, методологія, аналіз кейсів, результати дослідження, висновки та рекомендації. Бібліографічний список оформлено відповідно до вимог, присутні посилання на нормативні акти й стандарти. Представлено практично орієнтовану методику, що включає етапи: аналіз контексту, визначення зацікавлених сторін, оцінка ризиків та впливу на права користувачів, формування вимог, технічна інтеграція, пілотне впровадження. Методика враховує суміжні правові й етичні аспекти.

Недоліки

Доцільно було більше уваги приділити аналізу відомих корпоративних кодексів організацій кібербезпеки. Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Донцов Єгор Андрійович заслуговує присвоєння кваліфікації “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною та кібернетичною безпекою”.

Рецензент: доцент кафедри
Технічних систем кіберзахисту

к.т.н, доцент _____ Юрій ПЕПА
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 83 стор., 22 рис., 8 табл., 61 джерел.

Метою роботи є розробка методичних підходів та практичних механізмів формування політик інформаційної безпеки та їх технічна інтеграція в системи моніторингу для ефективного захисту гібридних інфраструктур.

Об'єкт дослідження – процес розробки, впровадження та підтримки політик кібербезпеки в сучасних організаціях.

Предмет дослідження – моделі та методи, що визначають ефективність розробки політик кібербезпеки в сукупності етичних, правових і технічних аспектів.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, синтезу, моделювання, метод балансу інтересів – для дослідження компромісу між вимогами кібербезпеки організації та правами користувачів, контент-аналіз – для дослідження текстів політик, кодексів етики та регламентів.

Короткий зміст роботи. У роботі досліджено нормативно-правову базу та міжнародні стандарти, що включають етичну, нормативну та технічну складову розробки політик інформаційної безпеки; розроблено пілотний проєкт "Політики допустимого використання"; реалізовано технічний моніторинг виконання політики шляхом налаштування правил виявлення інцидентів (Brute Force, Data Exfiltration) у системі IBM QRadar. Розроблено методику, яка на відміну від існуючих, враховує етичні, правові та технічні аспекти як взаємопов'язані елементи єдиної системи управління інформаційною безпекою.

Галузь застосування. Розроблені підходи можуть бути використані при побудові комплексних систем захисту інформації (КСЗІ) та операційних центрів безпеки (SOC) на підприємствах, що використовують гібридну модель роботи.

КЛЮЧОВІ СЛОВА: ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, SIEM-СИСТЕМА, IBM QRADAR, AUP, СОЦІАЛЬНА ІНЖЕНЕРІЯ, УПРАВЛІННЯ РИЗИКАМИ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 83 pages, 22 figures, 8 tables, 61 sources.

The purpose of the work is to develop methodological approaches and practical mechanisms for forming information security policies and their technical integration into monitoring systems for the effective protection of hybrid infrastructures.

Object of research is the process of developing, implementing, and supporting cybersecurity policies in modern organizations.

Subject of research is models and methods that determine the effectiveness of cybersecurity policy development in terms of ethical, legal, and technical aspects.

Research methods. To solve the above scientific problem, the work uses methods of system analysis, synthesis, modeling, and experimental methods.

Brief content of research. The work examines the regulatory framework and international standards that include ethical, regulatory, and technical components of information security policy development; a pilot project, “Acceptable Use Policy,” has been developed; Technical monitoring of policy implementation has been implemented by configuring incident detection rules (Brute Force, Data Exfiltration) in the IBM QRadar system. A methodology has been developed which, unlike existing ones, takes into account ethical, legal, and technical aspects as interrelated elements of a unified information security management system.

Field of research. The developed approaches can be used in building complex information security systems (CISS) and security operations centers (SOC) at enterprises that use a hybrid operating model.

KEYWORDS: INFORMATION SECURITY POLICY, SIEM SYSTEM, IBM QRADAR, AUP, SOCIAL ENGINEERING, RISK MANAGEMENT.

ЗМІСТ

ВСТУП

Актуальність теми. У цифровий час, де відбувається масова цифровізація та зростання кіберзагроз, стабільне функціонування державних та комерційних організацій безпосередньо залежить від ефективності їхніх систем кібербезпек. Але, як показують провідні світові звіти, наприклад Verizon DBIR 2025, переважна більшість інцидентів безпеки (понад 60%) спричинена не збоєм технологій, а людським фактором – помилками персоналу, неефективним управлінням або порушенням процедур. Тому головним фундаментом будь-якої системи захисту є не лише технічні засоби, а й чіткі, дієві та комплексні політики безпеки.

Політики потрібні для того, щоб: встановити “правила” для співробітників та систем; регламентувати дії персоналу в звичайних та не звичайних ситуаціях та забезпечити відповідність компанії вимогам законодавства (зокрема, GDPR та Закону України “Про захист персональних даних”).

Однак, більшість існуючих політик є або формальними, застарілими документами, або, навпаки, фокусуються лише на одному аспекті, ігноруючи інші. Виникає розрив між трьома ключовими компонентами: технічні, правові та етичні аспекти.

Таким чином, розробка методичних підходів до створення політик кібербезпеки, які б комплексно інтегрували та збалансували, технічні, правові та етичні аспекти, є надзвичайно актуальною науково-практичною задачею.

Теоретичним підґрунтям дослідження стали праці провідних вітчизняних вчених. Стратегічні виклики та тенденції розвитку кібербезпеки в Україні досліджували Д. В. Дубов та М. А. Ожеван [1]. Питання технічного та соціотехнічного захисту інформації ґрунтовно висвітлені у підручниках за редакцією В. Л. Бурячка [2], а також у працях О. К. Юдіна, О. Г. Корченка та Г. Ф. Конаховича [3]. Правові аспекти інформаційної безпеки та захисту даних детально проаналізовані А. І. Марущаком [4].

Однак, незважаючи на значний науковий доробок, питання комплексної інтеграції етичних норм у технічні політики та створення єдиних методичних підходів для сучасних гібридних середовищ потребують подальшого вивчення.

Мета роботи полягає у підвищенні рівня захищеності інформаційних систем шляхом розробки комплексної методики формування політик кібербезпеки та впровадження автоматизованих засобів контролю їх дотримання.

Для досягнення цієї мети необхідно виконати наступні **завдання**:

1. Проаналізувати нормативно-правову базу України та міжнародні стандарти у сфері розробки політик.
2. Визначити ключові етичні аспекти та проблеми балансу між безпекою організації та правами користувачів.
3. Провести аналіз практичних кейсів порушень безпеки, спричинених неефективними політиками.
4. Дослідити існуючі методи оцінки ефективності політик.
5. Розробити методику розробки та впровадження політик, що враховує етичні, правові та технічні вимоги.
6. Сформулювати рекомендації щодо інтеграції технічних методів захисту в політики та розробити приклад політики.

Об'єкт дослідження – процес розробки, впровадження та підтримки політик кібербезпеки в сучасних організаціях.

Предмет дослідження – моделі та методи, що визначають ефективність розробки політик кібербезпеки в сукупності етичних, правових і технічних аспектів.

Методи дослідження. Для досягнення поставленої мети у роботі використані методи:

– *теоретичні*: аналіз і узагальнення наукової літератури та нормативно-правових актів; систематизація підходів; порівняльний аналіз міжнародних стандартів;

– *емпіричні*: вивчення та аналіз кейсів порушень кібербезпеки; контент-аналіз документів;

– *прикладні*: методи моделювання; методи ризик-орієнтованого аналізу; обґрунтування застосування інструментів безпеки для технічної реалізації політик;

– *візуалізаційні:* побудова схем, моделей і таблиць для представлення результатів.

Наукова новизна дослідження полягає у розробці комплексного підходу до формування політик кібербезпеки в організаціях, який на відміну від існуючих, враховує етичні, правові та технічні аспекти як взаємопов'язані елементи єдиної системи управління інформаційною безпекою. Запропоновано методику розробки та оцінювання ефективності політик, що забезпечує баланс між вимогами кіберзахисту та правами користувачів..

Практичне значення одержаних результатів. Методика процесу може бути використана організаціями як покроковий алгоритм для створення нових або аудиту існуючих політик.

Галузь застосування. Розроблений алгоритм технічної інтеграції та шаблон "Політики допустимого використання" для умовної компанії можуть слугувати практичним посібником для фахівців з кібербезпеки, керівників IT-відділів та юридичних служб.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 28 лютого 2025 року.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ОСНОВИ РОЗРОБКИ ПОЛІТИК КІБЕРБЕЗПЕКИ

Ефективна система захисту інформації в сучасній організації неможлива без надійного теоретичного та нормативного підґрунтя. Політики кібербезпеки виступають ключовим елементом управління, що трансформує стратегічні цілі бізнесу в конкретні правила та процедури. У цьому розділі було досліджено сутність та призначення політик, проведено їх класифікацію відповідно до міжнародних стандартів, а також проаналізовано нормативно-правову базу та етичні аспекти, що формують контекст для їх розробки.

1.1 Класифікація політик безпеки (організаційні, технічні, поведінкові)

Насамперед політика кібербезпеки є частиною політики інформаційної безпеки. Політика інформаційної безпеки - це сукупність директив, положень, правил і практик, що визначають, як організація управляє, захищає та поширює інформацію [5]. У ній йдеться про всі види інформації: паперову, цифрову та усну. Політика кібербезпеки у свою чергу спрямована на захист інформації в кіберпросторі, а також на захист комп’ютерних систем, мереж та даних від кібератак та несанкціонованого доступу.

Авторитетний підручник “Management of Information Security” поглиблює це розуміння. Автори Уітмен та Меттord (Whitman & Mattord) дають такі визначення [6]:

– політика (policy) – це “у бізнесі, заява про наміри керівництва, призначення для скерування та регулювання поведінки співробітників в організації”.

– політики інформаційної безпеки (information security policies) – це “письмові інструкції, надані керівництвом, які інформують співробітників та інших на робочому місці про належну поведінку щодо використання інформації та інформаційних активів”.

Ці визначення підкреслюють ключовий, але часто ігнорований аспект: політика – це не технічний, а в першу чергу управлінський інструмент.

Цю всеохоплюючу, управлінську роль політики наочно ілюструє модель “Мішень” (“Bull’s-eye model”), представлена у підручнику Уітмена та Метторда (рис. 1.1) [6].

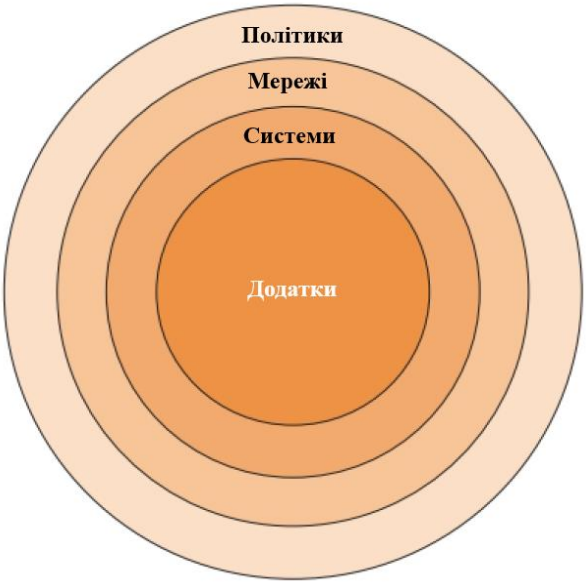


Рис. 1.1. Модель “Мішень” (Адаптовано за джерелом [6])

У цій моделі “Policies” (Політики) формують зовнішній, найвищій шар. Це візуально демонструє, що політики є первинним інструментом, який встановлює правила для всіх внутрішніх рівнів захисту: “Networks” (Мереж), “Systems” (Систем) та “Applications” (Додатків).

Таким чином, головне призначення політики – продемонструвати волю та підтримку вищого керівництва. Як зазначають Уітмен та Метторд, політика є “фундаментальною основою” (essential foundation) ефективної програми безпеки, оскільки вона “пояснює волю керівництва (explain the will of the

organization's management) у контролі за поведінкою співробітників” [6]. Це підтверджується цитатою NIST, наведеною у тому ж джерелі, де вказується що успіх програми захисту залежить від “ставлення керівництва (attitude of management)… Ваша головна відповідальність – задати тон (set the tone)” [6].

Отже, політика кібербезпеки виконує низку ключових функцій:

1. Встановлює “правила гри” та чіткі очікування для всіх співробітників.
2. Надає повноваження фахівцям з безпеки для впровадження технічних контролів та процедур.
3. Забезпечує основу для відповідності (Compliance) вимогам законодавства та стандартам.
4. Слугує “чек-листом” для проведення внутрішніх та зовнішніх аудитів.

На практиці неможливо створити єдиний всеосяжний документ, який би детально описував усі аспекти кібербезпеки – від стратегічних цілей до правил змін пароля. Такий документ був би нечитабельним та недієвим, оскільки він змішував би аудиторії: те, що важливо для вищого керівництва, відрізняється від того, що потрібно системному адміністратору.

Цю ієрархію наочно ілюструє модель “Піраміди” (Рис. 1.2), представлена у підручнику Уітмена та Меттorда [6].

Рис. 1.2. Ієрархія документів безпеки (Адаптовано за джерелом [6])

Ця модель структурує документи наступним чином:

Policies (Політики) знаходяться на вершині піраміди. Це високорівневі документи, санкціоновані вищим керівництвом, що задають загальний напрямок.

Standards (Стандарти) це обов'язкові до виконання специфікації, які деталізують, що саме має бути зроблено для дотримання політики.

Guidelines (Настанови): Це рекомендовані практики та поради про те, як досягти відповідності стандартам.

Procedures (Процедури): Це детальні покрокові інструкції, які описують, як саме виконувати конкретне завдання.

Самі політики також поділяються на типи. Для їх класифікації звертаємось до стандартів NIST. Як NIST SP 800-14 [7] (на нього спирався підручник [6], але на даний момент стандарт **відкладений**) так і **чинний** NIST SP 800-12 Rev. 1 [5] пропонують ідентичну 3-рінвеву класифікацію політик:

- **Program Policy** (Політика програми);
- **Issue-specific Policy** (Політика з конкретних питань);
- **System-specific Policy** (Політика для конкретних систем).

Program Policy. Ця політика є вищого рівня, вона використовується для створення програм та визначення напрямку безпеки. Вона також розподіляє ресурси для їх впровадження в організації.

В таблиці 1.1. наведені основні компоненти [5] політики програми.

Таблиця 1.1

Основні компоненти Program Policy (Політики програми)

Program Policy	
Мета	Описує цілі програми безпеки, такі як цілісність, доступність та конфіденційність
Сфера застосування	Чітко визначає, які ресурси (об'єкти, апаратне, ПЗ, персонал) захищає політика
Обов'язки	Призначає відповідальних за виконання політики
Відповідність	Визначає вимоги до відповідності та "використання штрафних санкцій та дисциплінарних стягнень" за порушення

Практичним прикладом такої політики є шаблон “Program Management Policy” [8] від SANS Institute [9], який слугує загальною рамкою для всіх інших політик.

Issue-Specific Policy. Вона розробляється для актуальних та проблемних питань організації на основі рекомендацій політики інформаційній безпеці. Вона повинна надавати зрозумілі інструкції та рекомендації щодо належного використання систем співробітникам організації. На відміну від політик програм, політики щодо конкретних питань необхідно регулярно переглядати через часті технологічні зміни в організації.

В таблиці 1.2 наведені основні компоненти [5] політик з конкретних питань.

Таблиця 1.2

Основні компоненти Issue-Specific Policy (Політики з конкретних питань)

Issue-Specific Policy	
Формування проблеми	Визначає саму проблему, релевантні терміни, умови та обґрунтування політики. Наприклад, дає чітке визначення “неофіційного програмного забезпечення”.
Позиція Організації	Чітко викладає рішення керівництва щодо сформульованої проблеми (наприклад, чи щось заборонено, чи дозволено за певних умов, хто і як надає винятки).
Сфера застосування	Пояснює, *де, як, коли, до кого* (наприклад, лише штатні співробітники, а не підрядники) та *до чого* (наприклад, лише до ресурсів в офісі чи й до тих, що використовуються вдома) застосовується ця політика.
Ролі та обов’язки	Призначає, *хто* і за що відповідає в рамках цієї політики. Наприклад, хто має повноваження надавати дозвіл на використання приватного ПЗ, а хто відповідає за моніторинг.
Відповідність	Описує неприпустимі порушення та **наслідки** (санкції, штрафи) за таку поведінку. Може визначати конкретний відділ, відповідальний за моніторинг дотримання.
Контактні особи	Вказує, до кого в організації слід звертатися за додатковою інформацією, роз'ясненнями чи допомогою. Рекомендується вказувати посади (напр., системний адміністратор), а не конкретні імена.

Типові приклади для **Issue-Specific Policy** наведені в табл. 1.3.

Таблиця 1.3

Приклади політик

Назва політики	**Що регулює**
Internet Access (Доступ до Інтернету)	– хто саме в організації матиме доступ до Інтернету; – які типи систем можна підключати до мережі; – які типи інформації дозволено передавати через мережу; – вимоги до автентифікації.
Приватність електронної пошти (Email Privacy)	– яка інформація (листи) збирається та зберігається; – як саме ця інформація використовується; – можливість моніторингу пошти з боку керівництва (для бізнес-цілей, запобігання вірусам, образливому контенту тощо); – рівень приватності, який може очікувати співробітник; – обставини, за яких пошта може бути прочитана.
Використання власних пристроїв (Bring Your Own Device - BYOD)	– дозвіл на використання особистих пристроїв (телефонів, ноутбуків) у робочих цілях; – виклики безпеці та приватності через різноманітність ОС та конфігурацій; – специфічні вимоги до пристрою (напр., шифрування, антивірус); – правила поведінки, яких має дотримуватись користувач для отримання доступу до ресурсів.
Соціальні мережі (Social Media)	– захист організації та її співробітників під час використання соцмереж (навіть якщо у компанії немає офіційної присутності); – встановлення чітких “правил поведінки” (guidelines) для користувачів; – визначення рівня суворості: від повної заборони на робочих ресурсах до дозволеного доступу з певними обмеженнями.

Практичне підтвердження цієї класифікації та приклади таких політик можна знайти у збірці шаблонів SANS Institute [9]. SANS надає безліч документів, які відповідають категорії Issue-Specific Policy (ISSP), регулюючи поведінку користувачів. Серед них:

– Email Management Policy (Політика управління поштою) [10];

– Mobile Device Policy (Політика управління мобільними пристроями) [11];

– Artificial Intelligence Acceptable Standard (Стандарт допустимого використання ШІ) [12].

Цікаво відзначити, що SANS часто називає ці документи “Стандартами”, а не “Політиками” (наприклад, Acceptable Use Standard [13]). Це не суперечить нашій моделі, а, навпаки, поглиблює її, чітко слідуючи моделі “Піраміди” (Рис. 1.2). Політика Програм встановлює намір, а ці документи (ISSP) функціонують як обов’язкові “Стандарти”, які деталізують правила поведінки для конкретного питання.

System-specific Policy. Ці політики визначають дозволені дії та налаштування безпеки для конкретних систем (наприклад, фаєрволів, серверів, ОС), забезпечуючи реалізацію загальних цілей інформаційної безпеки організації. Вони деталізують вимоги до безпеки, базуючись на загальних політиках і мають регулярно переглядатися відповідно актуальним процедурам.

Стандарт NIST 800-12 [5] та підручник Уітмана та Маттorда [6] пояснюють, що SysSP часто має дворівневу модель:

Security Objectives/Managerial Guidance (Управлінська частина): Це високорівневий опис того, що має бути зроблено. Наприклад, “Фаєрвол повинен блокувати весь вхідний трафік, крім портів 80 і 443”.

Operational Security Rules/Technical Specifications (Технічна частина): Це конкретні налаштування та інструкції, які реалізують управлінську волю. Наприклад скріншот конфігурації фаєрволу.

Технічна реалізація цих політик відбувається через специфічні механізми. Підручник та NIST 800-12 виділяють два основні методи

Access Control Lists (ACLs) (Списки контролю доступу): Це набір правил, які визначають, хто, до чого, коли і як може отримати доступ. Вони є основою безпеки у більшість операційних системах (Рис. 1.3 та 1.4).

Configuration Rules (Правила конфігурації): Це інструкції для таких систем, як фаєрволи, IDPS та проксі-сервери, ще регулюють потік даних. Наочним прикладом є набір правил для фаєрволу Palo Alto (Рис. 1.5).

Наприклад, вікно налаштувань “Локальна політика безпеки” у Windows (Рис. 1.6) є прямим візуальним прикладом інтерфейсу для управління System-Specific Policy.

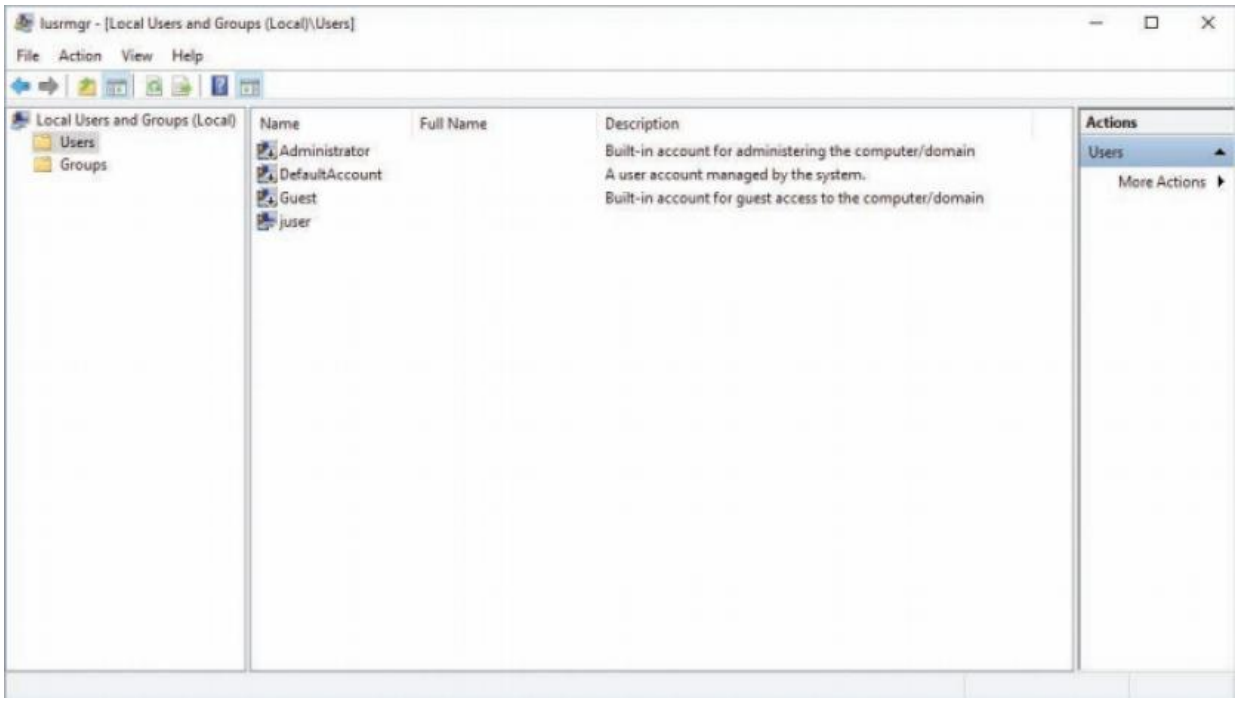


Рис. 1.3. Приклад Users ACL у Windows (Джерело: [6])

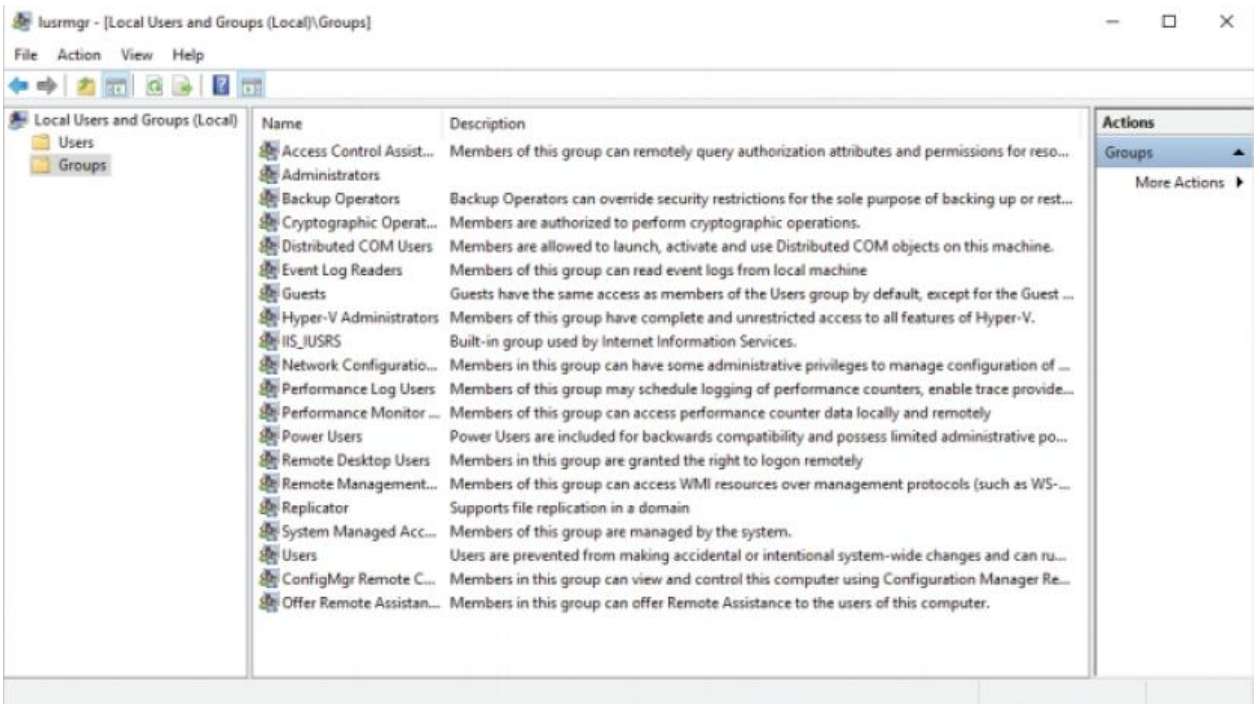


Рис. 1.4. Приклад Groups ACL у Windows (Джерело: [6])

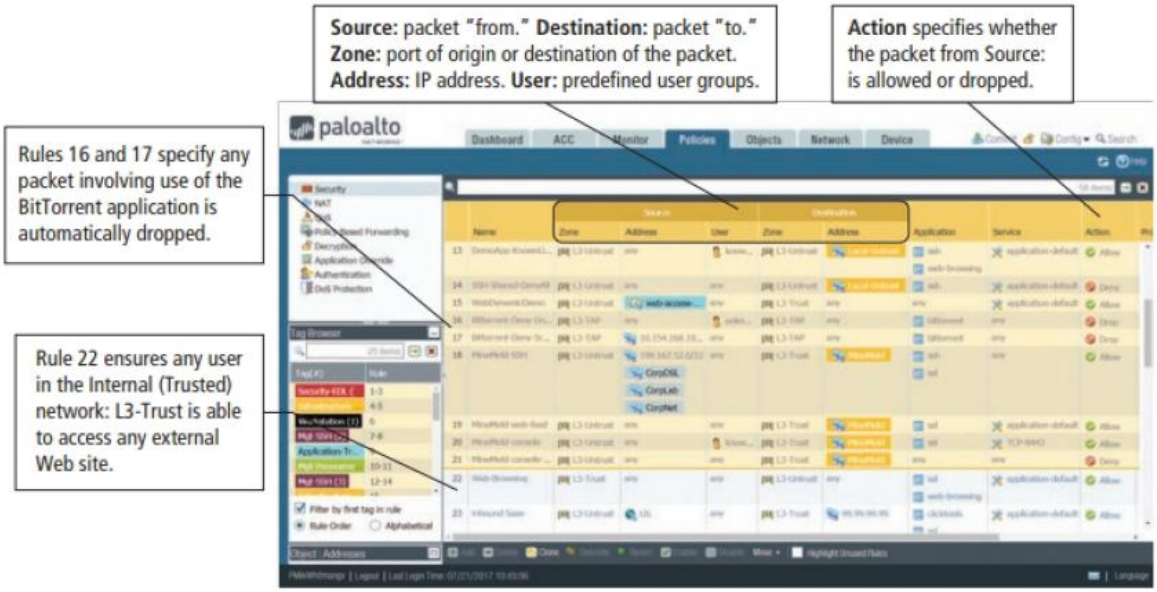


Рис. 1.5. Приклад правил конфігурації фаєрволу [6])

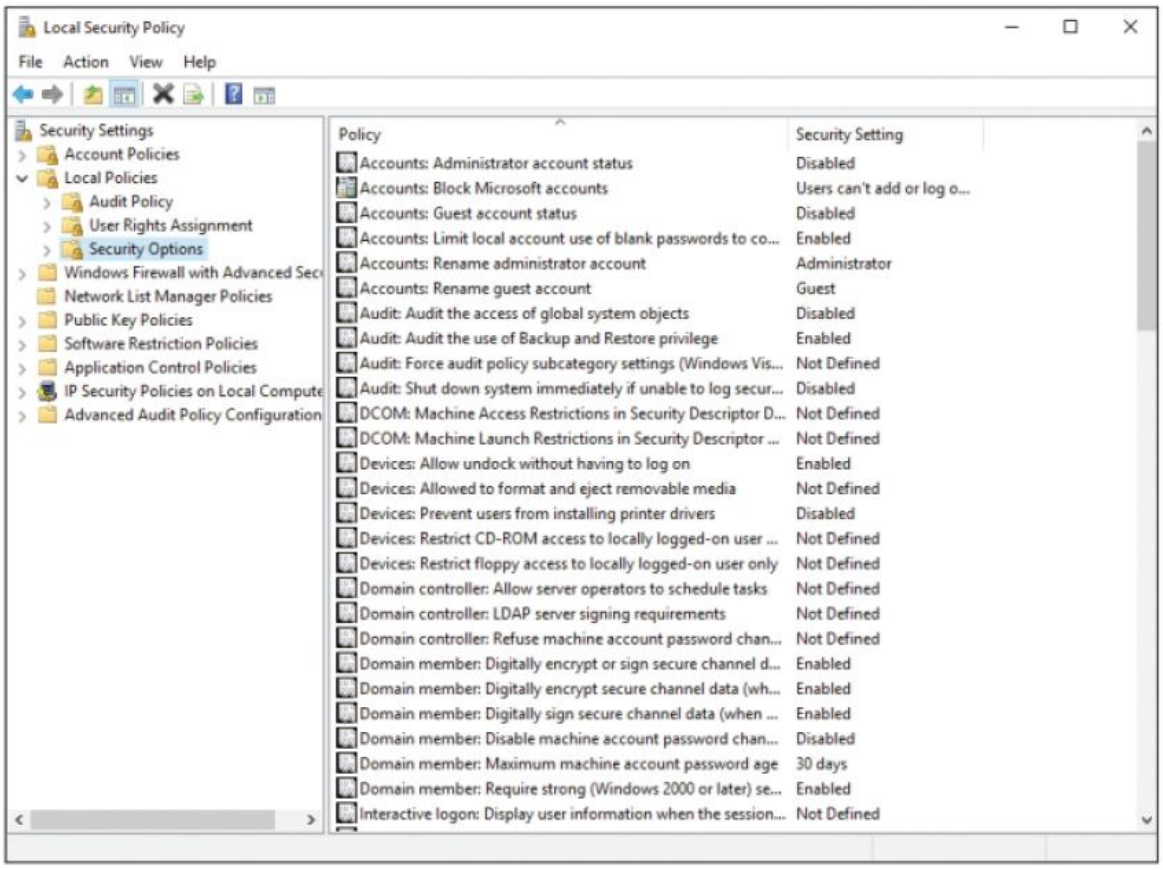


Рис. 1.6. Локальна політика безпеки у Windows (Джерело: [6])

На завершення, важливо зазначити, що фундаментальні стандарти (такі як NIST SP 800-14) висувають загальні вимоги до всіх трьох типів політик. Вони повинні бути: Supplemented (Доповнені стандартами та процедурами), Visible (Видимими/Доступними), Supported by Management (Підтримані керівництвом) і, найголовніше, Consistent (Узгодженими) з іншими директивами, законами та організаційною культурою.

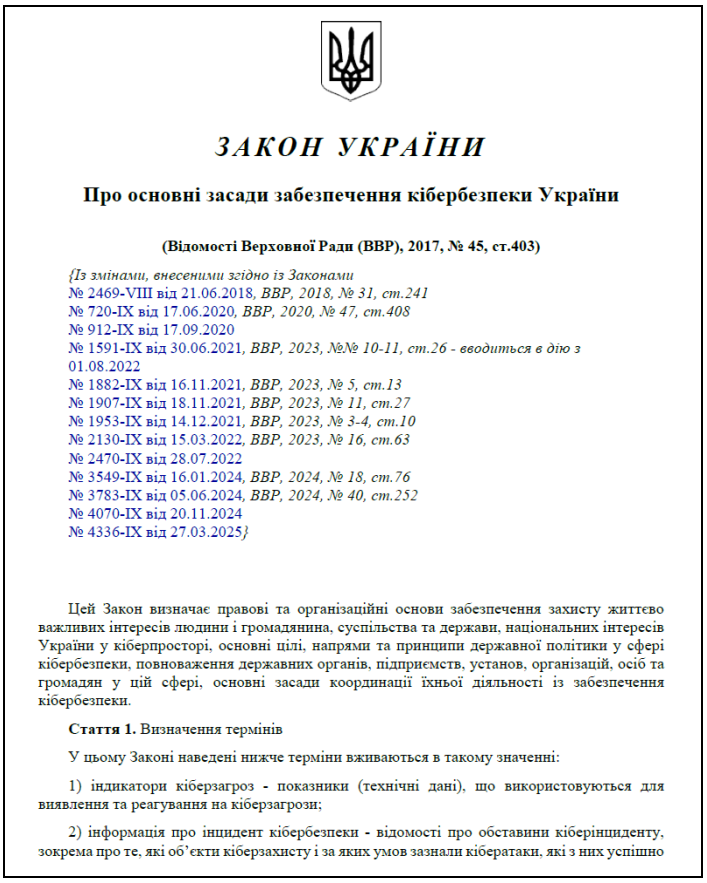
Саме ця остання вимога – узгодженість із законодавством – формує правові рамки для розробки будь-якої політики. Детальний аналіз цих рамок проводиться у наступному підрозділі.

1.2 Нормативно-правова база України та міжнародні стандарти

Як було зазначено у попередньому підрозділі, однією з фундаментальних вимог до всіх типів політик є їхня узгодженість із законами та організаційною культурою. Політика ніколи не повинна суперечити закону. У цьому підрозділі буде проаналізовано ключові нормативні документи, які формують правову основу для розробки політик кібербезпеки в Україні.

Національне законодавство України.

Основним документом є Закон України “Про основні засади забезпечення кібербезпеки України” № 2163-VIII від 5 жовтня 2017 року [14] (рис. 1.7). Цей закон визначає правові та організаційні основи захисту національних інтересів у кіберпросторі, встановлює цілі, напрями та принципи державної політики, а також повноваження і обов’язки державних органів та організацій. Він вводить ключові поняття, такі як “кібербезпека”, “кіберзахист”, “кібератака” та “об’єкти критичної інфраструктури”, створюючи єдиний термінологічний апарат.



ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

(Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)

{Із змінами, внесеними згідно із Законами
№ 2469-VIII від 21.06.2018, *ВВР, 2018, № 31, ст.241*
№ 720-IX від 17.06.2020, *ВВР, 2020, № 47, ст.408*
№ 912-IX від 17.09.2020
№ 1591-IX від 30.06.2021, *ВВР, 2023, №№ 10-11, ст.26 - вводиться в дію з* 01.08.2022
№ 1882-IX від 16.11.2021, *ВВР, 2023, № 5, ст.13*
№ 1907-IX від 18.11.2021, *ВВР, 2023, № 11, ст.27*
№ 1953-IX від 14.12.2021, *ВВР, 2023, № 3-4, ст.10*
№ 2130-IX від 15.03.2022, *ВВР, 2023, № 16, ст.63*
№ 2470-IX від 28.07.2022
№ 3549-IX від 16.01.2024, *ВВР, 2024, № 18, ст.76*
№ 3783-IX від 05.06.2024, *ВВР, 2024, № 40, ст.252*
№ 4070-IX від 20.11.2024
№ 4336-IX від 27.03.2025*}*

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

2) інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно

Рис. 1.7. Закон України “Про основні засади забезпечення кібербезпеки України” № 2163-VIII від 5 жовтня 2017 року

Важливо, що **Стаття 5[1]** вимагає від держорганів та об’єктів критичної інфраструктури “призначати відповідальну особу” з питань кіберзахисту. Це прямо впливає на Program Policy, оскільки один з її ключових компонентів (як наведено в табл. 1.1) – це “Обов’язки”. Крім того, **Стаття 6** зобов’язує посадових осіб, власників або розпорядників об’єктів критичної інфраструктури “повідомляти в установленому порядку про кіберінциденти”. Це означає, що їхня Issue-Specific Policy – а саме політика реагування на інциденти – повинна бути розроблена з урахуванням цих законодавств.

Ще одним із найважливіших законів є Закон України “Про захист персональних даних” №2297-VI від 1 червня 2010 року [15] (Рис. 1.8). Закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і

громадянина, зокрема права на втручання в особисте життя, у зв'язку з обробкою персональних даних.

ЗАКОН УКРАЇНИ

Про захист персональних даних

(Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481)

{Із змінами, внесеними згідно із Законами
№ 4452-VI від 23.02.2012, *ВВР, 2012, № 50, ст.564*
№ 5491-VI від 20.11.2012, *ВВР, 2013, № 51, ст.715*
№ 245-VII від 16.05.2013, *ВВР, 2014, № 12, ст.178*
№ 383-VII від 03.07.2013, *ВВР, 2014, № 14, ст.252*
№ 1170-VII від 27.03.2014, *ВВР, 2014, № 22, ст.816*
№ 1262-VII від 13.05.2014, *ВВР, 2014, № 27, ст.914*
№ 316-VIII від 09.04.2015, *ВВР, 2015, № 26, ст.218*
№ 675-VIII від 03.09.2015, *ВВР, 2015, № 45, ст.410*
№ 1774-VIII від 06.12.2016, *ВВР, 2017, № 2, ст.25*
№ 2168-VIII від 19.10.2017, *ВВР, 2018, № 5, ст.31*
№ 324-IX від 03.12.2019, *ВВР, 2020, № 11, ст.63*
№ 524-IX від 04.03.2020, *ВВР, 2020, № 38, ст.279*
№ 1089-IX від 16.12.2020
№ 1357-IX від 30.03.2021, *ВВР, 2021, № 29, ст.234*
№ 1667-IX від 15.07.2021
№ 1723-IX від 08.09.2021, *ВВР, 2021, № 50, ст.395*
№ 1907-IX від 18.11.2021, *ВВР, 2023, № 11, ст.27*
№ 1914-IX від 30.11.2021, *ВВР, 2023, № 4-5, ст.11*
№ 1962-IX від 15.12.2021, *ВВР, 2023, № 2, ст.6*
№ 1971-IX від 16.12.2021
№ 2075-IX від 17.02.2022, *ВВР, 2023, № 15, ст.52*
№ 2347-IX від 01.07.2022
№ 2438-IX від 19.07.2022 - *щодо набрання чинності див.* пункт 2
№ 2494-IX від 29.07.2022
№ 3585-IX від 22.02.2024
№ 3980-IX від 19.09.2024
№ 4170-IX від 19.12.2024
№ 4240-IX від 12.02.2025*}*

{У тексті Закону слова "володілець бази персональних даних" і "розпорядник бази персональних даних" у всіх відмінках і числах замінено відповідно словами "володілець

Рис. 1.8. Закон України "Про захист персональних даних" №2297-VI від 1 червня 2010 року

Цей Закон диктує зміст майже всіх політик, що стосуються людей, та декілька про технічні політики. Ось декілька ключові пункти наведені в табл. 1.4.

Таблиця 1.4

Ключові пункти Закону України «Про захист персональних даних»

Пункт	**Опис**	**Вплив**
Принцип “Мети” (Стаття 6)	Закон вимагає, щоб “Мета обробки персональних даних має бути сформульована”	Issue-Specific Policy (наприклад, “Політика моніторингу” або “Політика BYOD”) і є тим документом, який формулює цю мету. Не можна просто моніторити співробітників; потрібно мати політику, яка пояснює навіщо (напр., “для запобігання витоку комерційної таємниці”).
Принцип “Прозорості” (Стаття 6)	Обробка має здійснюватися “відкрито і прозоро”	Політика не може бути таємною. Співробітники повинні бути ознайомлені з нею.
Принцип “Згоди” (Стаття 6, 11)	“Не допускається обробка... без її згоди”, крім випадків, визначених законом. “Згода” є першою і головною підставою для обробки.	Це найголовніша вимога до будь-якої ISSP. Якщо впроваджується моніторинг пошти, політика повинна містити механізм отримання “добровільного волевиявлення” (згоди) від співробітника.
Права співробітника (Стаття 8)	Співробітник (суб'єкт даних) має право знати про мету обробки , отримувати інформацію про умови надання доступу та відкликати згоду.	Політика має бути написана так, щоб реалізувати ці права. Вона має бути чіткою “інструкцією” для співробітника.
Обов'язок нерозголошення (Стаття 10)	Закон зобов'язує працівників не допускати розголошення персональних даних, які їм було довірено	Це дає пряме юридичне обґрунтування для створення політик Acceptable Use Policy та Confidentiality Policy (Політики конфіденційності) і застосування санкцій за їх порушення.
Принцип “Захисту” (Стаття 24)	Закон зобов'язує володільців “забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки”	Це є правовою підставою для впровадження всіх “технічних” політик. Впроваджування SysSP (фаєрволи, ACLs, шифрування) не просто тому, що це “добра практика”, а тому, що Закон України вимагає забезпечити технічний захист даних.

Діяльність у сфері кібербезпеки також регулюється низкою підзаконних актів та стратегічних документів:

– Стратегія кібербезпеки України [16]: Затверджена Указом Президента України, вона визначає пріоритети, цілі та шляхи їх досягнення на національному рівні.

– Закони України: “Про критичну інфраструктуру” [17], “Про державну службу спеціального зв'язку та захисту інформації України” [18] та “Про захист інформації в інформаційно-телекомунікаційних системах” [19] створюють додаткові регуляторні рамки.

– Постанови Кабінету Міністрів України (КМУ): Низка постанов деталізує вимоги до кіберзахисту [20], зокрема:

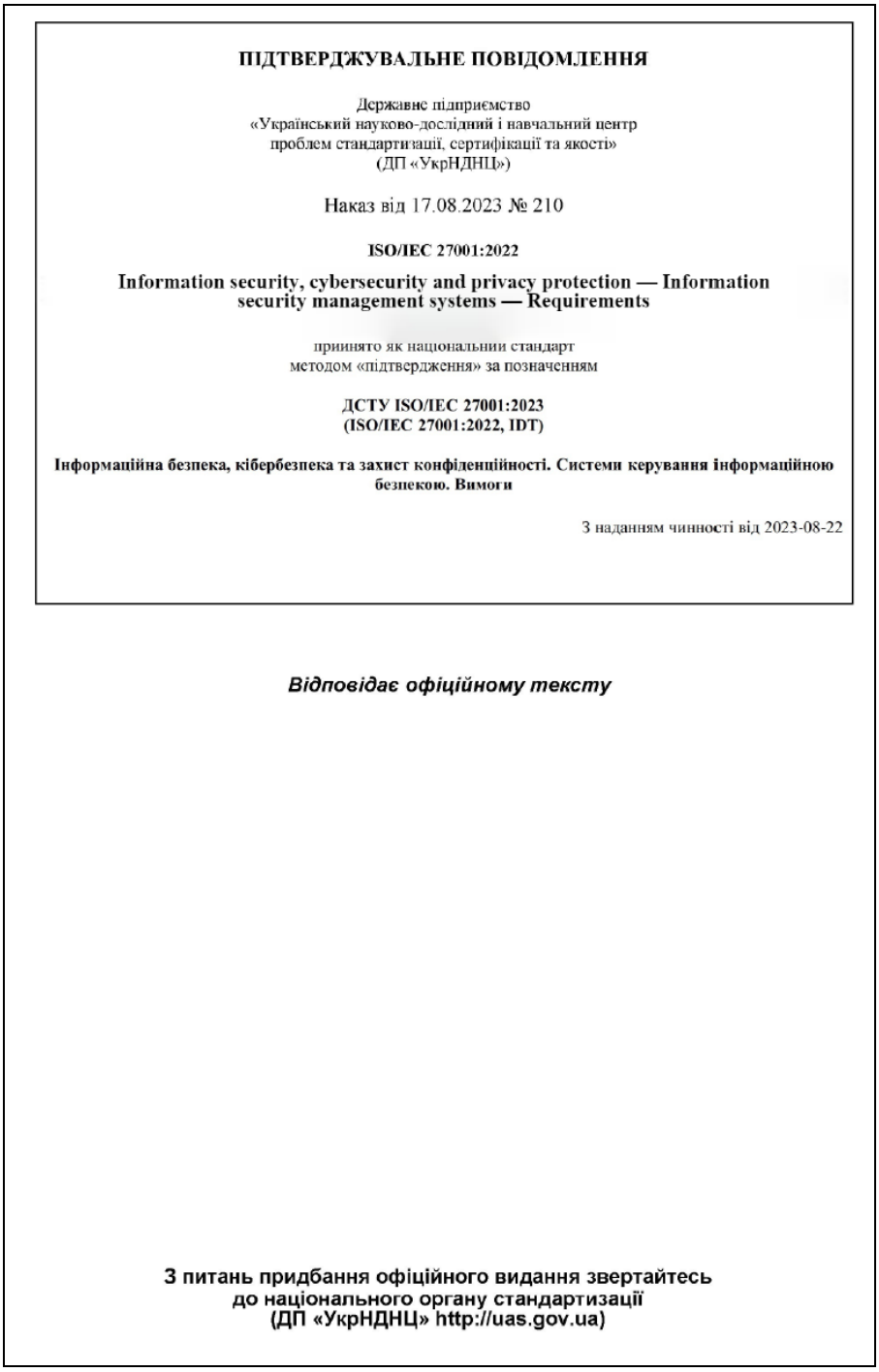
  – Постанова КМУ № 518 “Про затвердження Загальних вимог до кіберзахисту об’єктів інформаційної інфраструктури” [21].

  – Постанова КМУ № 943 [22] та № 1109 [23], що регулюють питання об'єктів критичної інформаційної інфраструктури.

– Накази Адміністрації Держспецзв’язку: Цей орган видає нормативні документи [20], що встановлюють технічні та організаційні вимоги до захисту інформації, координації дій під час інцидентів та оцінку стану захищеності державних ресурсів.

Державні стандарти України (ДСТУ).

Ключовим документом у цій категорії є ДСТУ ISO/IEC 27001:2023 “Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги” [24]. Як видно з підтверджувального повідомлення (рис. 1.9), цей стандарт прийнятний в Україні “методом “підтвердження”, що означає, що його текст **є ідентичним** міжнародному стандарту ISO/IEC 27001:2022 (рис. 1.10).



ПІДТВЕРДЖУВАЛЬНЕ ПОВІДОМЛЕННЯ

Державне підприємство
«Український науково-дослідний і навчальний центр
проблем стандартизації, сертифікації та якості»
(ДП «УкрНДНЦ»)

Наказ від 17.08.2023 № 210

ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

прийнято як національний стандарт
методом «підтвердження» за позначенням

ДСТУ ISO/IEC 27001:2023
(ISO/IEC 27001:2022, IDT)

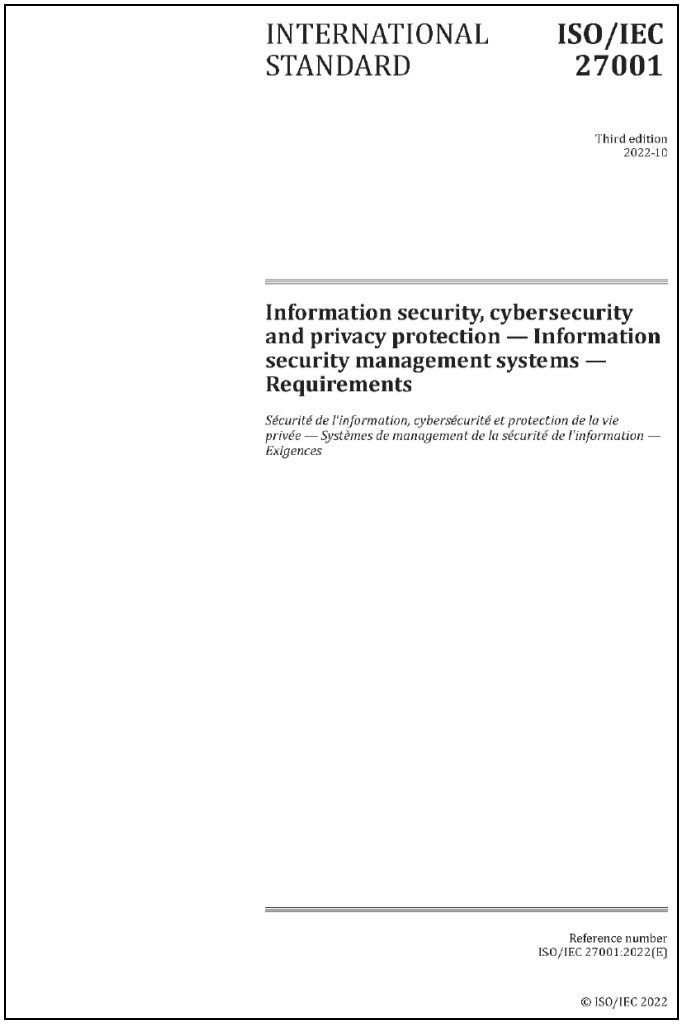
Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги

З наданням чинності від 2023-08-22

Відповідає офіційному тексту

З питань придбання офіційного видання звертайтесь до національного органу стандартизації (ДП «УкрНДНЦ» http://uas.gov.ua)

Рис. 1.9. Підтверджувальне повідомлення ДСТУ ISO/IEC 27001:2023


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

Рис. 1.10. Обкладинка ISO/IEC 27001:2022

Цей стандарт є “золотим стандартом” для побудови та сертифікації Системи Управління Інформаційною Безпекою (СУІБ) в організації. Він важливий тим, що він не просто рекомендує, а жорстко вимагає наявності та належного управління політиками.

Ця вимога з’являється у стандарті у двох ключових місцях:

Як вимога до керівництва (Розділ 5.2) [24]: Стандарт прямо вимагає, щоб “Вище керівництво” (Top management) встановило, впровадило політику інформаційної безпеки. Ця політика повинна: “відповідати меті організації” (si appropriate to the purpose of the organization); “включати цілі… або забезпечувати основу для їх встановлення” (includes information security

objectives… or provides the framework…); “включати зобов’язання задовольняти відповідні вимоги” (includes a commitment to satisfy applicable requirements).

Як конкретний контроль (Додаток А.5.1) [24]: У Додатку А стандарт надає перелік контролів безпеки. Контроль А.5.1 “Policies for information security” чітко вимагає, щоб політики (як загальна, так і тематичні): “були визначені (defined)”; “схвалені керівництвом (approved by management)”: “опубліковані та донесені персоналу (published, communicated to … relevant personnel)”; “переглянуті через заплановані проміжки часу (reviewed at planned intervals)”.

Таким чином, ДСТУ ISO/IEC 27001 не лише підтверджує необхідність Program Policy, але й встановлює чіткі, обов’язкові до виконання вимоги до її життєвого циклу: від створення та схвалення до комунікації та регулярного перегляду.

Міжнародні стандарти та GDPR.

NIST (Національний інститут стандартів і технологій США).

Хоча стандарти NIST (National Institute of Standards and Technology) є обов’язковими в основному для урядових установ США, вони де-факто стали найкращою практикою для індустрії в усьому світі. Як було зазначено у підпункті 1.2, фундаментальний стандарт NIST SP 800-12 Rev. 1 надав нам чітку 3-рівневу класифікацію політик. Водночас найактуальнішим документом, який визначає управлінський підхід, є NIST Cybersecurity Framework (CSF) 2.0 [25], представлений у 2024 році.

Його основна суть – це “таксономія високорівневих результатів кібербезпеки”. Простим словами, це не детальна інструкція, а структурований список цілей, яких організація має досягти, щоб належним чином керувати ризиками безпеки.

Ключові характеристики:

– не є прескриптивним: Фреймворк не наказує, як саме досягати результатів. Він лише описує бажаний стан (наприклад, “доступ до активів контролюється”);

– універсальність: Він розроблений для організацій будь-якого розміру, сектору чи рівня зрілості;

– добровільність: Це добровільний ресурс, хоча деякі урядові політики можуть вимагати його використання;

– глобальність: Він не прив’язаний до конкретної країни чи технології.

Головна мета CSF 2.0 – допомогти організаціям “краще розуміти, оцінювати, визначати пріоритети та комунікувати” свої зусилля з управління ризиками безпеки.

Він надає “спільну мову” для спілкування про ризики. Це дозволяє технічним спеціалістам, менеджерам та вищому керівництву (наприклад, раді директорів) однаково розуміти стан захищеності організації.

Фреймворк допомагає організації відповісти на ключові питання:

1. Розуміти та Оцінювати: “Який наш поточний стан кібербезпеки?”
2. Визначати пріоритети: “Яким ми хочемо бачити наш стан? Які кроки є найважливішими?”
3. Комунікувати: “Як ми можемо пояснити наші потреби в ресурсах та наші досягнення керівництву та партнерам?”

Фреймворк також створений для того, щоб інтегрувати ризики кібербезпеки в загальну систему управління ризиками підприємства (ERM).

CSF 2.0 складається з трьох основних компонентів:

1. **Ядро CSF (CSF Core).**

NIST CSF 2.0 побудований навколо 6-ти Функцій (Functions) (рис. 1.11). Ці функції – це найвищий рівень таксономії, що описує ключові стовпи управління ризиками кібербезпеки. Варто зазначити, що функція “**GOVERN (GV) – УПРАВЛІННЯ**” є новою і найважливішою функцією у CSF 2.0. Вона слугує фундаментом для всіх інших п’яти функцій [21].

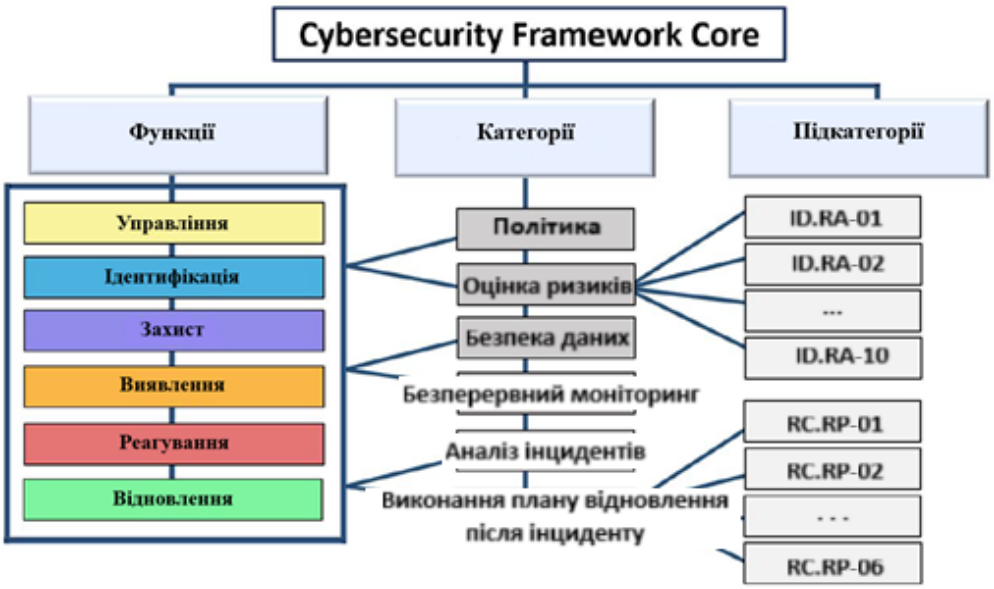


Рис. 1.11. Структура ядра CSF 2.0

1. **GOVERN (GV) – УПРАВЛІННЯ**: Стратегія очікування та політика організації щодо ризиків кібербезпеки встановлені, донесені (communicated) та моніторяться.

2. **IDENTIFY (ID) – ІДЕНТИФІКАЦІЯ**: Поточні ризики кібербезпеки організації зрозумілі.

3. **PROTECT (PR) – ЗАХИСТ**: Засоби захисту для управління ризиками кібербезпеки організації використовуються.

4. **DETECT (DE) – ВИЯВЛЕННЯ**: Можливі атаки та компрометації виявляються та аналізуються.

5. **RESPOND (RS) – РЕАГУВАННЯ**: Вживаються дії щодо виявленого інциденту кібербезпеки.

6. **RECOVER (RC) – ВІДНОВЛЕННЯ**: Активи та операції, що постраждали від інциденту, відновлюються

Кожна з цих 6 функцій поділяється на Категорії (Categories), які уточнюють бажані результати. Таблиця 1.5 деталізує всі 6 функцій та категорії, на які вони поділяються.

Таблиця 1.5

Функції та їх категорії

Функція	**Ідентифікатор**	**Категорія (Опис)**
GOVERN (GV) – УПРАВЛІННЯ	GV.OC	Organizational Context (Організаційний контекст)
	GV.RM	Risk Management Strategy (Стратегія управління ризиками)
	GV.RR	Roles, Responsibilities, and Authorities (Ролі, обов'язки та повноваження)
	GV.PO	Policy (Політика)
	GV.OV	Oversight (Нагляд)
	GV.SC	Cybersecurity Supply Chain Risk Management (Управління ризиками ланцюга постачання)
IDENTIFY (ID) – ІДЕНТИФІКАЦІЯ	ID.AM	Asset Management (Управління активами)
	ID.RA	Risk Assessment (Оцінка ризиків)
	ID.IM	Improvement (Вдосконалення)
PROTECT (PR) – ЗАХИСТ	PR.AA	Identity Management, Authentication, and Access Control (Управління ідентифікацією, автентифікацією та контролем доступу)
	PR.AT	Awareness and Training (Обізнаність та навчання)
	PR.DS	Data Security (Безпека даних)
	PR.PS	Platform Security (Безпека платформ)
	PR.IR	Technology Infrastructure Resilience (Стійкість технологічної інфраструктури)
DETECT (DE) – ВИЯВЛЕННЯ	DE.CM	Continuous Monitoring (Безперервний моніторинг)
	DE.AE	Adverse Event Analysis (Аналіз несприятливих подій)
RESPOND (RS) – РЕАГУВАННЯ	RS.MA	Incident Management (Управління інцидентами)
	RS.AN	Incident Analysis (Аналіз інцидентів)
	RS.CO	Incident Response Reporting and Communication (Звітність та комунікація при реагуванні)
	RS.MI	Incident Mitigation (Пом'якшення наслідків інциденту)
RECOVER (RC) – ВІДНОВЛЕННЯ	RC.RP	Incident Recovery Plan Execution (Виконання плану відновлення після інциденту)
	RC.CO	Incident Recovery Communication (Комунікація під час відновлення)

Кожна категорія деталізується у Підкатегоріях (Subcategories). Усього у CSF 2.0 їх 106.

Наприклад, давайте розглянемо категорію GV.PO (Policy), яка є найбільш релевантною у дослідженні. Вона має дві підкатегорії [25].

1. **GV.PO-01**: “Політика для управління ризиками кібербезпеки встановлюється на основі організаційного контексту, стратегії кібербезпеки та пріоритетів, а також доноситься (communicated) та забезпечується її виконання (enforced)”. Простими словами: GV.PO-01 вимагає, не просто написати документ, а й офіційно його затвердити, роздати всім співробітникам і попередити, що його виконання є обов’язковим.

2. **GV.PO-02**: “Політика для управління ризиками кібербезпеки переглядається (reviewed), оновлюється (updated), доноситься та забезпечується її виконання для відображення змін у вимогах, загрозах, технологіях та організаційній місії”. Простими словами: GV.PO-02 вимагає, щоб політика була “живим документом”, який регулярно перевіряється на актуальність і адаптується до нових законів, загроз і технологій.

2. Профілі CSF (CSF Profiles).

Профілі – це механізм для опису стану організації за допомогою Ядра.

– Поточний профіль (Current Profile): Описує поточний стан організації (які результати вже були досягнуті).

– Цільовий профіль (Target Profile): Описує бажаний стан (які результати організація хоче досягти для виконання місії).

Аналіз розриву між цими двома профілями допомагає створити план дій для покращення.

3. Рівні CSF (CSF Tiers).

Рівні описують “суворість” або зрілість процесів управління ризиками організації. Вони показують, як організація розглядає ризики. Існує 4 рівні:

– Рівень 1 (Tier 1): Partial (Частковий): Процеси хаотичні (ad hoc), реактивні, з обмеженою обізнаністю про ризики.

– Рівень 2 (Tier 2): Risk-Informed (Інформований про ризики): Керівництво затверджує практики, але вони можуть не бути впроваджені по всій організації.

– Рівень 3 (Tier 3): Repeatable (Повторювані): Практики формально затверджені як політика, процеси є повторюваними та регулярно переглядаються.

– Рівень 4 (Tier 4): Adaptive (Адаптивний): Організація постійно вдосконалюється, адаптується до загроз і використовує прогнозування.

Таким чином, аналіз найсучаснішого міжнародного фреймворку NIST CSF 2.0 підтверджує ключову тезу нашої роботи. Введення нової функції GOVERN (УПРАВЛІННЯ) та виділення окремої категорії GV.PO (Policy) ставить розробку, донесення, виконання та регулярний перегляд політик в самий центр ефективного управління кібербезпекою. Це доводить, що політика є фундаментальним управлінським інструментом, а не просто формальним документом.

GDPR (Загальний регламент про захист даних ЄС) .

Особливе місце у нормативно-правовій базі посідає Загальний регламент про захист даних (GDPR) Європейського Союзу. На відмінну від стандартів ISO та NIST, які є рекомендаційними фреймворками, GDPR – це обов’язковий до виконання закон, який встановлює одні із найсуворіших у світі правил захисту даних [26] (рис.1.12).

Ключова особливість GDPR для України – це його екстериторіальний принцип дії. Регламент застосовується не лише до компаній, зареєстрованих в ЄС, але й до будь-якої організації у світі, незалежно від її місцезнаходження, якщо вона:

– пропонує товари чи послуги (навіть безкоштовно) громадянам, які перебувають на території ЄС;

– моніторить поведінку громадян, поки вони перебувають на території ЄС.

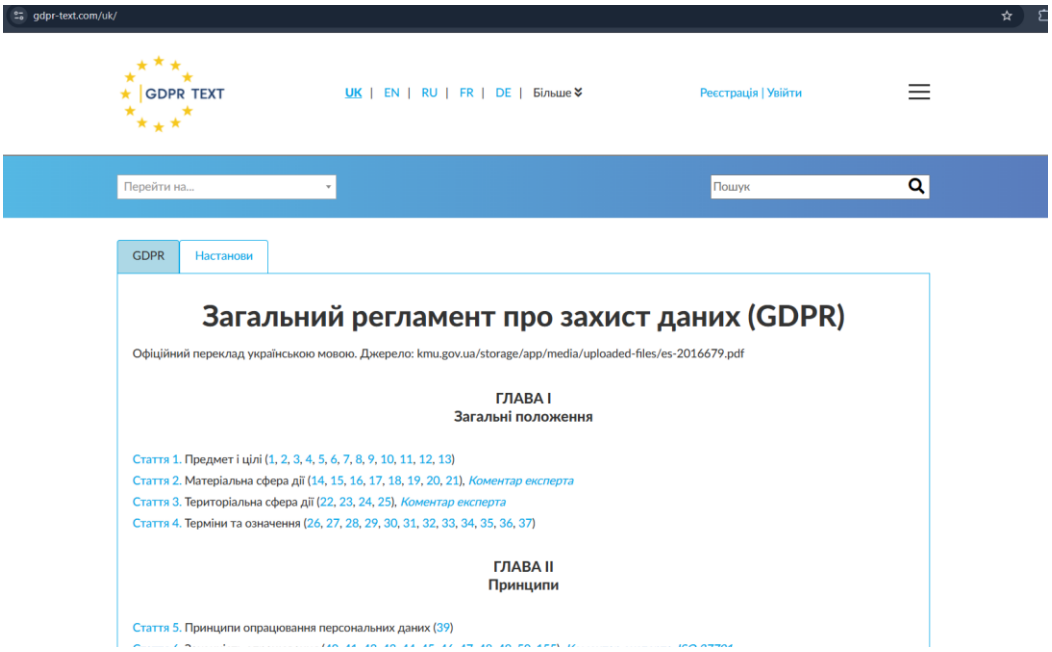


Рис. 1.12. Сайт “gdpr-text.com/uk” [22] з GDPR на українській мові

Для українського бізнесу це означає, що будь-яка IT-аутсорсингова компанія, яка працює з європейськими клієнтами та обробляє їхні дані, e-commerce сайт, що продає товари в ЄС, або маркетингова агенція, що аналізує поведінку користувачі з ЄС, автоматично зобов’язана виконувати вимоги GDPR.

Також, Регламент виступає потужним правовим драйвером, який змушує компанії створювати та впроваджувати дуже детальні, чіткі та дієві політики. Він встановлює фундаментальні принципи, кожен з яких безпосередньо диктує зміст ISSP (Поведінкових політик):

1. Законність, справедливість і прозорість: Компанія зобов’язана “прозоро” інформувати суб'єктів даних про те, які дані, чому і як вона обробляє. Це вимагає наявності чіткої, загальнодоступної та зрозумілої політики конфіденційності.

2. Обмеження метою: Дані можна збирати лише для “конкретних, чітких і законних цілей” і не можна обробляти у спосіб, несумісний із цими цілями. Це накладає жорсткі обмеження, наприклад, на Email Monitoring Policy

(Політику моніторингу пошти) — компанія не може моніторити пошту “про всяк випадок”, а лише для конкретної, законної та заздалегідь визначеної мети.

3. Мінімізація даних: Організації повинні збирати лише той обсяг даних, який є абсолютно необхідним для досягнення заявленої мети. ISSP мають відображати цей принцип, забороняючи збір надлишкової інформації.

4. Технічний та організаційний захист: GDPR вимагає впровадження “відповідних технічних та організаційних заходів” для захисту даних, таких як шифрування, контроль доступу та регулярні аудити. Це є прямим юридичним обґрунтуванням для розробки SysSP, які описують ці заходи.

5. Підзвітність: Це один із найважливіших принципів. Організація повинна бути здатною не просто відповідати вимогам, а й продемонструвати свою відповідність. Наявність детального, затвердженого та впровадженого набору політик (Політика згоди, Політика реагування на витік даних, Політика захисту даних) є головним доказом такої підзвітності для регуляторів.

Враховуючи, що штрафи за порушення GDPR можуть сягати 20 мільйонів євро або 4% світового річного обороту компанії, ігнорування цих вимог несе прямі фінансові та репутаційні ризики. Це перетворює розробку політик з “рекомендації” (як у NIST чи ISO) на критичну юридичну необхідність для українських компаній, інтегрованих у глобальний ринок.

1.3 Етичні аспекти формування політик кібербезпеки: баланс між безпекою та правами користувачів

Розробка політик кібербезпеки не є виключно технічним чи юридичним завданням. Вона неминуче торкається етичних аспектів, оскільки створює фундаментальний конфлікт інтересів:

– право організації на безпеку. Організація має законне право захищати свою власність, комерційну таємницю та інфраструктуру.

– право користувача (співробітника) на приватність. Співробітник, навіть на робочому місці, має право на певний рівень особистого простору та невтручання в особисте життя, що гарантується Конституцією України (ст. 32) [27].

Технічні політики (SysSP), такі як моніторинг мереж, та поведінкові політики (ISSP), як-от політика електронної пошти, дають організації потужні інструменти для контролю. Питання полягає в тому, де проходить етична межа між не обхідним захистом та надмірним стеження.

Необхідність політики, яка б встановлювала цей баланс, ідеально ілюструє кейс, наведений у підручнику Уітмена та Метторда [6]:

Співробітник поводиться неналежно – переглядає заборонені сайти або читає чужу пошту. Інший працівник, обурений такою поведінкою, подає до суду, вважаючи робоче середовище ворожим. Оскільки компанія не має політики, що забороняє такі дії, будь-які санкції проти порушника можуть спричинити судовий позов. Суд ухвалює рішення на користь постраждалого, присуджує компенсацію, і компанія зазнає банкрутства. В іншому варіанті керівник звільняє порушника, але той подає позов за незаконне звільнення, адже не існувало офіційної політики, що визначає цю поведінку як порушення. Суд знову стає на бік працівника, і компанія знову втрачає фінансову спроможність.

Цей кейс демонструє класичну “етико-правову пастку”, спричинену відсутністю політики:

– якщо компанія **НЕ діє** (не монітрорить/не звільняє): Вона несе юридучну відповідальність за створення “ворожого робочого середовища” для інших співробітників.

– якщо компанія **ДІЄ** (звільняє): Вона несе юридичну відповідальність за “незаконне звільнення”, оскільки співробітник формально не порушував жодних задокументованих правил.

Вирішення цієї дилеми – і є той самий “баланс” – досягається через розробку політики, що базується на прозорості та інформованій згоді.

Саме тут етичні вимоги повністю збігаються з правовими. Як було детально проаналізовано у таблиці 1.3, Закон України “Про захист персональних даних” вимагає [15]:

– Принцип “Мети” (Стаття 6): Мета обробки (наприклад, “моніторинг для запобігання витоку таємниці”) має бути чітко сформульована;

– Принцип “Згоди” (Стаття 6, 11): Обробка, як правило, не допускається без згоди;

– Принцип “Прозорості” (Стаття 6): Обробка має бути “відкритою і прозорою”;

– Права співробітника (Стаття 8): Співробітник має право знати про мету обробки.

Таким чином, ISSP (наприклад, “Політика допустимого використання” або “Політика моніторингу”) і є цим ключовим етичним інструментом. Етичною вважається не та політика, яка не моніторить (ставлячи під загрозу всю компанію, як у кейсі), а та, яка чесно, відкрито і заздалегідь повідомляє співробітникам:

1. Що саме моніториться (напр., “корпоративна пошта”, “відвідані веб-сайти”).

2. Що не моніториться (напр., “особисті месенджери на вашому BYOD-пристрої”).

3. Навіщо це робиться (мета, напр., “запобігання витоку комерційної таємниці” та “забезпечення безпечного робочого середовища”).

4. Які наслідки порушення (санкції).

Отримуючи підпис співробітника про ознайомлення з такою політикою, організація забезпечує інформовану згоду. Це знімає етичний конфлікт: співробітник поінформований про “правила гри”, а компанія отримує юридичне та етичне право захищати свої активи. Сам так і досягається баланс між безпекою організації та правами користувачів.

Висновки до розділу 1

У цьому розділі було проаналізовано теоретичні, методологічні, правові та етичні основи політик кібербезпеки.

Політика кібербезпеки – це не просто технічний документ, а фундаментальний управлінський інструмент, який виражає волю керівництва та “задає тон” безпеці в організації. Існує чітка ієрархія документів (Політики, Стандарти, Настанови, Процедури). Самі політики класифікуються за 3-рівневою моделлю NIST на Program Policy (організаційні), Issue-Specific Policy (поведінкові) та System-Specific Policy (технічні).

Розробка політик жорстко регулюється. Закони України та міжнародні норми (як ДСТУ ISO 27001 та GDPR) встановлюють прямі вимоги до змісту політик, наявності відповідальних осіб та механізмів захисту даних.

Ключовим етичним викликом є баланс між безпекою та приватністю користувачів . Етична політика досягає цього балансу через механізми прозорості та інформованої згоди , які, у свою чергу, також вимагаються законодавством про захист персональних даних

РОЗДІЛ 2

АНАЛІЗ СУЧАСНОГО СТАНУ ФОРМУВАННЯ ТА ВПРОВАДЖЕННЯ ПОЛІТИК КІБЕРБЕЗПЕКИ

Теоретичні засади, розглянуті у попередньому розділі, окреслюють ідеальну модель управління безпекою. Однак практика показує, що реалізація політик часто стискається із суттєвими перешкодами. Метою цього розділу є аналіз реального стану впровадження політик кібербезпеки на основі міжнародної та вітчизняної статистики інцидентів. Будуть досліджені практичні кейси провалів у системах захисту, розглянуті існуючі методи оцінки ефективності політик та виявлені ключові проблеми інтеграції технічних, правових та етичних аспектів, що знижують рівень захищеності організацій.

2.1 Аналіз міжнародного та вітчизняного досвіду реалізації політик кібербезпеки

Аналіз міжнародного досвіду реалізацій політик кібербезпеки доцільно провести на основі найновішого та найавторитетнішого галузевого звіту – Verizon Data Breach Investigation Report (DBIR) 2025 року [28]. Цей звіт аналізує тисячі реальних інцидентів і чітко показує, що головні загрози лежать не в технологічній, а в людській та процесійній площині.

Ключовий висновок звіту DBIR (рис. 2.1) полягає в тому що 60% усіх інцидентів були пов’язані з “людським елементом” (human element). Це підтверджує що головні ризики лежать у поведінці персоналу.

Ця тенденція підтверджується й іншими глобальними звітами. Зокрема, звіт IBM “Cost of a Data Breach Report 2024” [29] вказує, що середня вартість витоку даних досягла рекордних 4.88 млн доларів. Microsoft Digital Defense Report 2024 [30] наголошує, що 99% атак на облікові записи можна запобігти

через MFA, а звіт “ENISA Threat Landscape 2024” [31] визначає соціальну інженерію як топ-загрозу для ЄС, що є критичним для українських компаній, які працюють на європейському ринку.

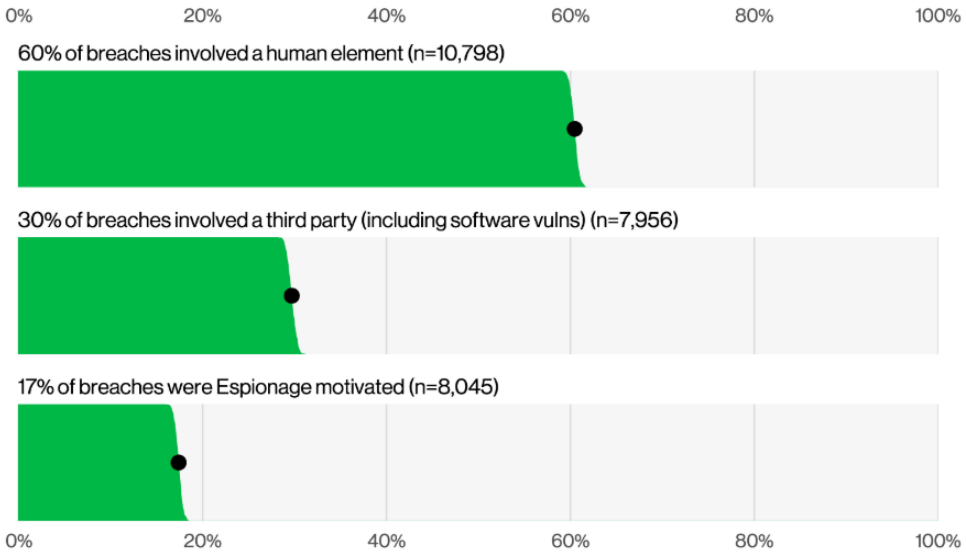


Рис. 2.1. Елементи успіху інцидентів (Джерело: [28])

Звіт детально розкриває цей “людський елемент”, виділяючи три основні моделі інцидентів, які є прямим наслідком провалу політик.

Провал поведінкових політик: Соціальна інженерія (Social Engineering).

Соціальна інженерія залишається домінуючим вектором атак (3,405 інцидентів з підтвердженою втратою даних [28]). Атаки майже завжди зовнішні (100%) і мають фінансову (55%) або шпигунські (52%) мотиви [28].

Ці атаки є прямим провалом ISSP, оскільки вони маніпулюють довірою персоналу. Звіт виділяє три основні техніки (див. рис. 2.2):

– Фішинг (Phishing, 57%). Це найпоширеніша дія. Провал політики тут полягає в тому, що програми обізнаності є неефективними. Рис. 2.3 це показує, що навіть в організаціях, які проводять симуляції фішингу, в середньому 5.7% співробітників все одно натискають на посилання. Це

доводить, що покладатися лише на поведінкову політику обізнаності – це провальна стратегія.

– Претекстінг (Pretexting, 30%). Це атаки, де зловмисник видає себе за довірену особу, що є основою для Business Email Compromise (BEC). Провал політики тут фінансово катастрофічний. Звіт 2025 року зазначає, що лише у 2024 році через BEC було переказано $6.3 мільярда. Це прямий **провал ISSP**, яка мала б вимагати процедури верифікації (наприклад, завжди підтверджувати зміну банківського рахунку телефонним дзвінком), але співробітники нею нехтують.

– Бомбардування запитами (Prompt bombing, 14%). Це новий небезпечний тренд, який DBIR виділяє у 2025 році. Це техніка обходу MFA (багатофакторної автентифікації), коли зловмисник маючи вкрадений пароль, "бомбардує" телефон користувача push-повідомленнями, сподіваючись, що той врешті-решт натисне "Approve". Це комплексний провал політик:

– **Провал ISSP**. Співробітники не навчені ніколи не схвалювати запити MFA, які вони не ініціювали.

– **Провал SysSP**. Системи (Access Control Management) не налаштовані так, щоб Блокувати акаунт після, наприклад, 5 запитів MFA за хвилину.

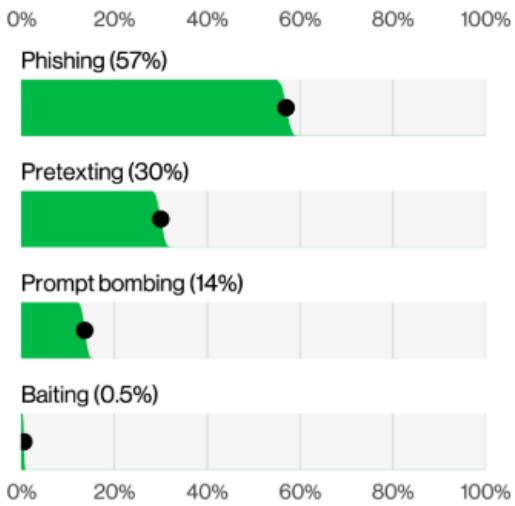


Рис. 2.2. Види соціальних дій в інцидентах (Джерело: [28])

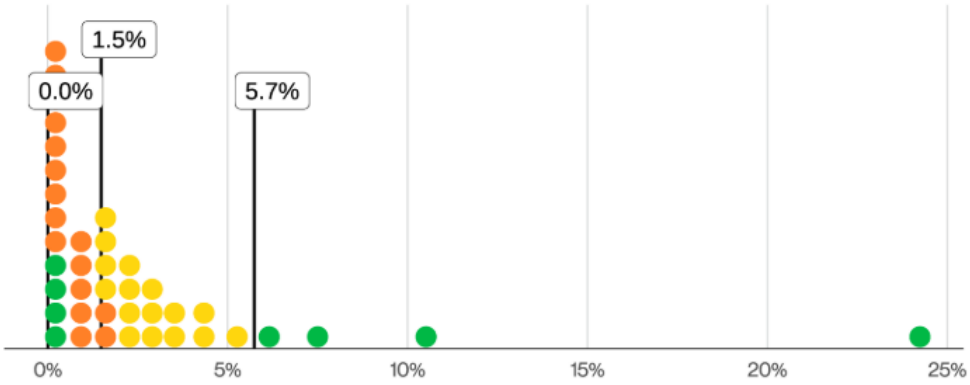


Рис. 2.3. Розподіл коефіцієнта кліків фішингової кампанії з моделювання за організаціями (кожна точка відповідає 193,58 організаціям) (Джерело: [28])

Провал поведінкових та технічних політик: Різні помилки (Miscellaneous Errors).

Цей розділ звіту аналізує ненавмисні помилки персоналу. Переважна більшість (98%) цих інцидентів спричинена внутрішніми акторами. Це також є провалом політик обізнаності та процедур. Типи помилок (рис. 2.4):

Неправильна доставка (Misdelivery, 49%): Це найпоширеніша помилка, колі співробітник надсилає конфіденційну інформацію (95% з якої – персональні дані) не тому адресату. Це недолік ISSP, яка мала б навчати персонал правилам поводження з даними.

Помилка конфігурації (Misconfiguration, 30%): Це друга за поширеністю помилка. Сюди відносяться неправильно налаштовані хмарні сховища або сервери. Це помилка SysSP, яка мала б чітко диктувати Configurations Rules (Правила конфігурації).

Сам звіт DBIR вказує, що ефективним рішенням для таких помилок є впровадження контролів за стандартом CIS Critical Security Controls (CIS Controls) v8 [32], зокрема контролю 14 (Security Awareness) та контролю 3 (Data Protection).

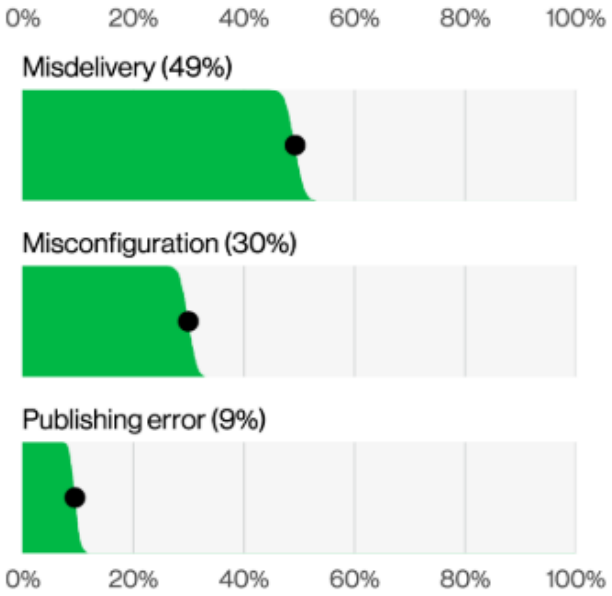


Рис. 2.4. Популярні види помилок (Джерело: [28])

Провал організаційних та технічних політик: Зловживання привілеями (Privilege Misuse).

Цей тип інциденту аналізує навмисні зловмисні дії з боку внутрішніх співробітників. Це комплексний провал на всіх рівнях: Program Policy (на етапі довіри та контролю) та SysSP (на етапі технічного обмеження доступу).

– Актори та Мотиви. Актор переважно внутрішній (90%). Мотиви – фінансові (89%) або шпигунство (10%) (рис.2.5). Текст звіту прямо вказує, що співробітники “крадуть дані... для власної фінансової вигоди, переходу до конкурента або для започаткування власного бізнесу” [28].

– Джерела зловживань (рис. 2.6). Звіт показує, що хоча звичайні “Кінцеві користувачі” (42%) є найбільшою групою, значну загрозу становлять привілейовані користувачі: “Системні адміністратори” (30%) та “Розробники” (10%). Це особливо небезпечно, оскільки вони мають вищий рівень доступу.

Цей тип атак процвітає через надмірну довіру та провал технічних політик (SysSP). Співробітникам надають більше доступу, ніж їм потрібно для роботи (“принцип найменших привілеїв” не дотримується). Сам звіт вказує на рішення – впровадження Access Control Management [CIS 6] та Account Management [CIS 5], що є основою SysSP.

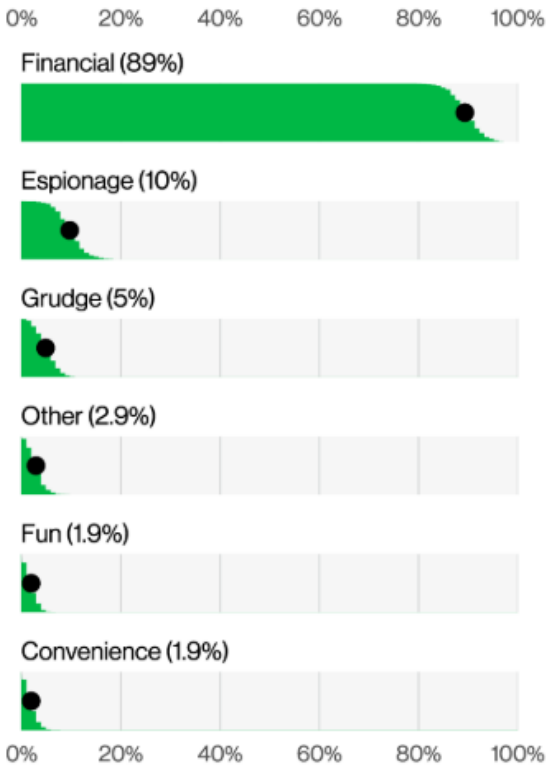


Рис. 2.5. Популярні мотиви акторів (Джерело: [28])

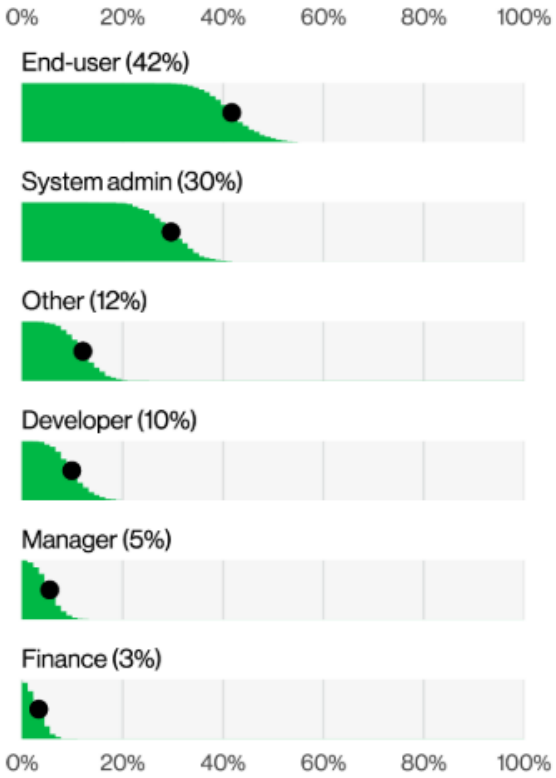


Рис. 2.6. Популярні джерела зловживань (Джерело: [28])

Таким чином, міжнародний досвід (DBIR 2025) чітко доводить, що організації зазнають збитків через системні збої в людських процесах та політиках. Провал може бути як ненавмисним (помилки Misdelivery) через нерозуміння ISSP, так і навмисним (Privilege Misuse) через провал у контролі доступу (SysSP).

Вітчизняний досвід.

Аналіз стану кібербезпеки в Україні, особливо в умовах повномасштабної війни, показує, що вітчизняні тренди збігаються з міжнародними: людський фактор та провал поведінкових політик залишаються ключовими вразливостями.

Найбільш повну картину надає “Річний звіт 2024” [33], опублікований Оперативним центром реагування на кіберінциденти (ОЦРК) Державного центру кіберзахисту (ДЦКЗ) Держспецзв’язку. Цей звіт ґрунтується на статистичних даних, зібраних Системою виявлення вразливостей і реагування на кіберінциденти та кібератаки (СВВ).

Протягом 2024 року СВВ зафіксувала майже 3 мільйони подій інформаційної безпеки, з яких 28 тисяч були визначені як “критичний”, що вимагали негайного втручання аналітиків. За результатами цього аналізу було опрацьовано 1042 повноцінних кіберінциденти.

Аналіз цих інцидентів дає чітке розуміння прогалин у політиках організацій.

1. **Домінування провалів ISSP.**

Звіт ДЦКЗ, так само як і DBIR, показує, що атаки, спрямовані на людей, є найефективнішими.

– Головний вектор атаки. “Ключовий висновок №2” звіту чітко вказує: “Використання скомпрометованих облікових записів та розповсюдження ШПЗ засобами електронної пошти є одними із найпоширеніших методів... для отримання первинного доступу” [33];

– Підтвердження у класифікації. Це підтверджується і на сторінці 15 звіту [33], де аналізуються найактивніші хакерські групи (UAC-0010, UAC-

0006, UAC-0050). Для кожної з них “Основним початковим вектором кібератак було розповсюдження ШПЗ засобами електронної пошти”;

– Технічна деталь. Звіт навіть чітко ідентифікує цю атаку за класифікацією MITRE ATT&CK як “T1566.001 Phishing: Spearphishing Attachment” (Цільовий фішинг із вкладенням).

Це є прямим, статистично підтвердженим доказом того, що ISSP в українських організаціях (переважно Урядовий та Оборонний сектори) масово не спрацьовують. Співробітники продовжують відкривати шкідливі вкладення, порушуючи базові правила кібергігієни.

2. Провал SysSP.

Звіт також показує, що провал поведінкової політики миттєво перетворюється на технічний інцидент.

– найбільша категорія зафіксованих подій (58.8%) – це “Шкідливий програмний код (Malicious Code)”;

– найбільша категорія опрацьованих кіберінцидентів – “02.04 Шкідливе підключення” (407 інцидентів). Це означає, що після фішингу шкідливе ПЗ успішно встановилося і почало “стукати” до командно-контрольного центру (C&C).

Це свідчить про провал SysSP. По-перше, засоби захисту кінцевих точок (EDR) не змогли заблокувати виконання ШПЗ. По-друге, політики фаєрволу (Configuration Rules) не змогли заблокувати вихідне “шкідливе підключення”.

Висновки збігаються з міжнародними. Аналіз офіційного звіту ДЦКЗ доводить, що найбільші ризики лежать у площині людського фактору.

Саме тому “Рекомендації” , які надає ДЦКЗ [33], є, по суті, набором вимог до розробки ефективних політик:

– “Використовуйте засоби захисту електронної пошти” та “Будьте обережні з електронними листами...” (пряма вимога до ISSP).

– “Використовуйте багатофакторну автентифікацію” (пряма вимога до SysSP контролю доступу).

– “Здійснюйте інвентаризацію активів...” (пряма вимога до Program Policy).

– “Налаштуйте логування” (пряма вимога до SysSP).

Таким чином, український досвід 2024 року підтверджує: провал ISSP (фішинг) залишається головним вектором атак, що призводить до технічних компрометацій (SysSP) .

2.2 Дослідження практичних кейсів порушень інформаційної безпеки через неефективні або відсутні політики

Якщо підпункт 2.1 показав статистику провалів політик (DBIR, ДЦКЗ), то цей підрозділ проаналізує механіку цих провалів на двох знакових кібератаках. Ці кейси ілюструють два основних типи збоїв: провал поведінкової політики через відсутність процедур та провал технічної політики через неефективне впровадження.

Атака на MGM Resorts (2023).

У вересні 2023 року одна з найбільших у світі мереж казино та готелів, MGM Resorts, зазнала катастрофічної кібератаки, яка призвела до повної зупинки операцій та фінансових збитків що оцінюються у понад $100 мільйонів.

Вектор атаки: Провал верифікації.

Як детально описує “Netwrix” [34], “Inszone Insurance” [35] та “Cobalt: Offensive Security Services” [36] атака була не складною технічно, а базувалася на соціальній інженерії. Зловмисники (група “Scattered Spider”) виконали 5 простих кроків:

1. Дослідження. Атакуючі знайшли співробітника MGM на LinkedIn.
2. Імітація. Вони обрали цього співробітника для імітації.
3. Дзвінок. Атакуючи подзвонили до IT-служби підтримки (help desk) MGM, видаючи себе за цього співробітника.

4. Провал політики. Вони “успішно переконали службу підтримки надати їм облікові дані для входу”.

5. Ескалація. Отримавши початковий доступ, зловмисники швидко отримали права адміністратора до систем Okta та Azure, проникли в мережу та залучили групу “ALPHV” для розгортання програми-вимагача.

Аналіз провалу політики.

Цей кейс є хрестоматійним прикладом катастрофічного провалу ISSP. Провал стався у процедурі верифікації IT-служби підтримки.

У компанії вартістю мільярди доларів була або відсутня, або не виконувалася чітка, обов’язкова ISSP (та пов’язана з нею процедури), яка б вимагала багаторівневої перевірки особи (наприклад, зворотній дзвінок на відомий номер, перевірка через менеджера, відеодзвінок) перед тим, як скидати пароль чи надавати доступ. Атака зайняла 10 хвилин і доводить висновок DBIR: людський елемент є найслабшою ланкою.

Наслідки провалу

Провал цієї однієї поведінкової політики призвів до ланцюгової реакції з нищівними наслідками:

– Фінансові. Загальні збитки склали приблизно $100 мільйонів, включаючи $84 мільйони втраченого доходу (через зупинку казино та готелів) та $10 мільйонів на реагування та відновлення (оплата послуг експертів, юристів тощо).

– Операційні. Повне припинення роботи. Вийшли з ладу ігрові автомати, цифрові ключі від номерів перестали працювати, системи бронювання та мобільні додатки “лягли”, було зупинено навіть електронну пошту та бронювання у ресторанах.

– Витік даних. Зловмисники заявили про викрадення 6 ТБ даних клієнтів, що включали імена, дати народження, номери телефонів, водійських посвідчень, а у деяких випадках – номери соціального страхування (SSN) та паспортів.

– Юридичні. Проти MGM було подано численні колективні позови (class-action lawsuits). Крім того, FTC (Федеральна торгова комісія США) та Рада з контролю за азартними іграми Невади розпочали власні розслідування щодо практик безпеки даних компанії.

Цікаво, що стаття водночас відзначає, що MGM мала “добре структурований план реагування на інциденти”. Їхнє “критичне рішення вимкнути системи”, хоч і спричинило фінансові втрати, запобігло поширенню ransomware по всій мережі. Це показує, що одна ISSP (реагування на інциденти) у них спрацювала, тоді як інша (верифікація особи) – повністю провалилася.

Висновок по кейсу: Кейс MGM доводить, що наявність складних технічних систем (Okta, Azure) є марною, якщо провалюється найпростіша поведінкова політика верифікації особистості.

Багатоетапний злам LastPass (2022).

Якщо кейс MGM ілюструє миттєвий крах через людську, помилку то злам LastPass – це приклад повільної, багатоетапної катастрофи, спричиненої фундаментальними провалами технічних політик. LastPass, один із найпопулярніших у світі менеджерів паролів, що обслуговує понад 30 мільонів користувачів, зазнав компрометації, яка підірвала саму суть його бізнесу.

Вектор атаки: Ланцюг провалів.

Згідно з дослідження “Breaking the Vault” (“Злам сховища”) [37] та деяких інших джерел [38, 39, 40], атака складається з двох основних етапів:

– Етап 1 (Провал ISSP). Атака почалася не зі штурму серверів LastPass, а зі зламу домашнього комп'ютера одного з чотирьох (!) старших інженерів DevSecOps. Зловмисник використав вразливість у “сторонньому програмному забезпеченні для медіа” (Plex), яке інженер використовував на своєму робочому пристрої. Це дозволило встановити keylogger (клавіатурний шпигун) і перехопити майстер-пароль інженера, коли той проходив багатофакторну автентифікацію (MFA).

– Етап 2 (Провал SysSP). Отримавши цей “ключ від усього”, зловмисник проник у хмарне сховище (AWS). Там він виявив вихідний код та

“вбудовані облікові дані у вигляді звичайного тексту”. Використовуючи ці вкрадені ключі, хакер отримав доступ до архівних бекапів (резервних копій) сховищ паролів клієнтів.

Аналіз провалу політик.

Цей кейс демонструє комплексний збій політик на всіх рівнях:

– Провал ISSP. Дослідження прямо зазначає: “LastPass не зміг впровадити сильні політики безпеки для співробітників, які працюють з дому” (“LastPass failed to implement strong security policies for employees working from their home network”). Політика віддаленої роботи (ISSP) дозволяла інженеру з найвищим доступом працювати на пристрої зі стороннім, вразливим ПЗ.

– Провал SysSP. Це стало катастрофічною причиною. Компанія, бізнес-модель якої – безпека, грубо порушила власні фундаментальні SysSP:

1. Провал Політики Шифрування. У бекапах містилися “незашифровані” дані клієнтів (імена, email, адреси) та метадані (URL-адреси сайтів). Це є грубим порушенням політики Data Security Policy, яка вимагає шифрування всіх даних у стані спокою.

2. Провал Політики Контролю Доступу. Облікові дані та ключі доступу до критичних бекапів були вбудовані у вихідний код у вигляді звичайного тексту.

3. Провал “Принципу найменших привілеїв”. Один скомпрометований інженер не повинен був мати доступу одночасно і до середовища розробки, і до ключів від хмарного сховища з бекапами

Наслідки провалу.

Наслідки виявилися нищівними, оскільки вони вдарили по самим клієнтам, які довіряли LastPass:

– Фінансові. Зловмисники використали вкрадені дані (метадані URL-адрес зі сховищ) для цілеспрямованих атак на клієнтів, які зберігали у LastPass ключі від криптовалютних гаманців. Станом на кінець 2023 року було підтверджено крадіжку $4.4 мільйонів у криптовалюті (із загальною сумою до $35 мільйонів) у понад 150 жертв.

– Втрата даних. Були вкрадені зашифровані сховища паролів (vaults) мільйонів користувачів. Хоча LastPass стверджує, що вони зашифровані, тепер зловмисники можуть “зламувати” їх в офлайн-режимі, використовуючи необмежений час, що ставить під загрозу кожен пароль, який там зберігався.

– Репутаційні. Провал був настільки фундаментальним, що провідні світові ЗМІ (Forbes, CNET, Wired) випустили статті з прямими рекомендаціями “припинити використання LastPass” , що фактично зруйнувало репутацію компанії.

Висновок по кейсу: Атака на MGM Resorts показала, що є критичною. Але злам LastPass доводить, що навіть якщо ISSP провалюється (злам інженера), компанія може вижити, якщо її SysSP працюють. Провал LastPass полягав у тому, що їхні технічні політики (шифрування, контроль доступу) були або відсутні, або не виконувалися, що й призвело до катастрофи.

2.3 Методи оцінки ефективності політик безпеки в організаціях

Як довели кейси з підпункту 2.2, наявність політики не реагує її ефективності. Найбільша проблема – це “політика на папері”, яка існує формально, але не виконується. Для того, щоб оцінити реальну дієвість політик, існують декілька ключових методів: аудит, оцінка зрілості, тестування та аналіз інцидентів.

Аудит відповідності – це формальний, систематичний процес перевірки, який має на меті дати об’єктивну відповідь на одне питання: “Чи відповідає те, що ми робимо насправді, тому, що ми написали у наших політиках?”. Політика може існувати, але якщо вона не виконується або виконується непослідовно, вона є не просто неефективно, а навіть небезпечною. Аудит – це інструмент для виявлення таких розривів між документацією та реальністю.

Цей метод є не просто “доброю практикою”, а прямою вимогою ключових міжнародних стандартів, які були проаналізовані у Розділі 1.

– ДСТУ ISO/IEC 27001:2023: Цей стандарт, який є основою для сертифікації Систем Управління Інформаційною Безпекою (СУІБ), містить у Додатку А (контроль А.5.36) “Compliance with policies, rules and standards for information security” [24]. Цей контроль вимагає від організацій, щоб відповідність її власним політикам та стандартам “регулярно переглядалася”.

– NIST CSF 2.0: Функція GOVERN (GV), яка була розглянута, включає категорію GV.OV (Oversight) (Нагляд) [25]. Ця категорія передбачає, що результати управління ризиками (тобто виконання політик) оцінюється для подальшого коригування стратегії.

Процес аудиту, незалежно від того, чи він проводиться внутрішніми силами чи зовнішніми аудиторами, зазвичай слідує чіткій структурі:

1. Планування (Planning). Це етап “що, де і як ми перевіряємо?”.

– Визначення обсягу. Аудитори вирішують, що саме вони перевірятимуть. Наприклад: “Аудит SysSP для серверної інфраструктури” або “Аудит ISSP щодо віддаленого доступу”.

– Визначення критеріїв. Це “еталон”, з яким будуть порівнювати. Критеріями є самі документи: Program Policy, SysSP “Політика управління оновленнями”, ISSP “Політика управління доступу” тощо.

2. “Польова робота” (Fieldwork)/Збір доказів. Це основний етап, де аудитори шукають об’єктивні докази виконання (або невиконання) політик. Вони не вірять на слово.

– Приклад 1: Аудит SysSP.

– Критерій: “Політика управління оновленнями” вимагає: “Усі критичні оновлення безпеки на серверах Windows мають бути встановленні протягом 72 годин з моменту їх випуску”;

– Процедура: Аудитор робить вибірку з 10 критичних серверів;

– Докази: аудитор запитує системні журнали (логи) серверів або звіти зі сканера вразливостей;

– Результат: Аудитор порівнює дати випуску патчів Microsoft з датами встановлення у логах.

– Приклад 2: Аудит ISSP.

– Критерій: “Політика управління доступу” вимагає: “Обліковий запис співробітника, що звільнився, має бути деактивованим протягом 1 години після завершення робочого дня”;

– Процедура: Аудитор бере список співробітників, звільнених за останній квартал (доказ від HR);

– Докази: Аудитор перевіряє логи Active Directory або іншої системи ідентифікації;

– Результат: Аудитор порівнює час звільнення з часом блокування акаунту.

3. Звітність (Reporting). Це фінальний етап де надається оцінка. Аудитор не дає суб’єктивної оцінки. Він надає список “невідповідностей”. Приклад звіту: “Виявлено велику невідповідність: обліковий запис співробітника А (звільнений 5 листопада) був активний ще 3 дні, що є прямим порушенням політики ISSP-Access-04”. Це створює критичний ризик Privilege Misuse, який можна побачити у звіті DBIR [28].

Аудит є ідеальним методом для оцінки формального виконання та дисципліни. Він гарантує, що затверджені правила виконуються, і є критично важливим для сертифікації (як ISO 27001). Але, його головний недолік у тому, що він оцінює лише відомі правила. Він не може оцінити, чи готова організація до невідомих загроз. Політика може на 100% відповідати аудиту (наприклад, всі паролі змінюються кожні 90 днів), але бути неефективною проти сучасної атаки (наприклад, фішингу, який краде цей пароль за 60 секунд).

Оцінка зрілості – це стратегічний метод, який оцінює не стільки зміст окремої політики, скільки загальну зрілість та ефективність усього процесу управління політиками в організації. Він допомагає зрозуміти, чи є політики

просто реактивними документами (написаними, бо “так треба”), чи вони є невід’ємною частиною корпоративної культури та управління ризиками.

Найсучаснішим та найпоширенішим інструментом для такої оцінки є Рівні (Tiers), представлені у NIST Cybersecurity Framework (CSF) 2.0 [25], який був детально проаналізований в підпункті 1.3. NIST CSF Tiers – це по суті, і є готова шкала для оцінки зрілості.

Процес оцінки зрілості, на відміну від аудиту (який шукає чіткі “так/ні”), є якісним аналізом.

1. Самооцінка. Організація (зазвичай IT-відділ, відділ безпеки та керівництво) проводить самооцінку, щоб визначити, який із чотирьох рівнів NIST Tiers найкраще описує їхній поточний стан.

2. Визначення Рівня. Команда аналізує свої процеси, пов’язані з політиками, і зіставляє їх з описом рівнів:

– Рівень 1: Partial (Частковий). Організація на цьому рівні має неефективні політики. Згідно з описом NIST , процеси управління ризиками (включаючи політики) є “хаотичними (ad hoc)” та “реактивними”. Обізнаність про ризики обмежена. Політики, якщо і існують, то лише “на папері”.

– Рівень 2: Risk-Informed (Інформований про ризики). Керівництво затверджує практики, але вони “можуть не бути впроваджені як політика по всій організації”. Тобто, політики існують, але їхнє виконання непослідовне.

– Рівень 3: Repeatable (Повторюваний). Це перший рівень справжньої ефективності. Згідно з NIST, тут практики “формально затверджені як політика (formally approved and expressed as policy)”. Процеси (як-от перегляд та оновлення політик GV.PO-02) є повторюваними та регулярно виконуються.

– Рівень 4: Adaptive (Адаптивний). Найвищий рівень. Організація “постійно вдосконалюється”, “адаптується” до нових загроз (як GenAI) і використовує прогнозування .

3. План розвитку/“Gap Analysis”. Після визначення поточного стану (наприклад, “ми на Рівні 2”), організація встановлює Цільовий профіль (Target Profile) (наприклад, “ми хочемо досягти Рівня 3”). На основі цього розробляється план дій (наприклад, “формалізувати всі ISSP, впровадити обов'язковий щорічний перегляд GV.PO-02”).

Оцінка зрілості за моделлю NIST CSF Tiers є потужним стратегічним інструментом. Вона дозволяє оцінити не окремий документ, а всю культуру управління політиками. Політика не може вважатися ефективною, якщо організація в цілому знаходиться на “хаотичному” Рівні 1, оскільки немає гарантій, що ця політика буде підтримуватися, оновлюватися чи виконуватися.

Практичне тестування – це група методів, яка оцінює ефективність політик шляхом симуляції реальних атак у контрольованому середовищі. На відміну від аудиту, який звіряється з “папером”, тестування перевіряє реальну стійкість систем та персоналу до атак. Цей метод ідеально підходить для оцінки як “поведінкових” (ISSP), так і “технічних” (SysSP) політик.

Симуляції (Оцінка ISSP).

Це тестування “людського елементу”, який згадувався у звітах DBIR та ДЦКЗ, є найслабшою ланкою. Найпоширеніший приклад – симуляція фішингу.

Етапи симуляції фішингу:

1. Планування. Команда безпеки (або зовнішній підрядник) створює реалістичний фішинговий лист (наприклад, “Терміново! Оновіть ваш пароль” або “Інофрмація про річний бонус”) і визначає цільову групу (наприклад, “вся компанія” або “тільки відділ бухгалтерії”).

2. Виконання та Збір метрик. Атака запускається. Спеціалізоване ПЗ автоматично збирає детальні метрики:

- Скільки співробітників відкрило лист?
- Скільки натиснуло на посилання?
- Скільки ввело свої облікові дані на фальшивій сторінці?

– Скільки співробітників повідомило про атаку (натиснуло кнопку “Report Phishing”)?

3. Оцінка ефективності. Організація отримує чіткий, кількісний показник (KPI) ефективності своєї ISSP (Політики обізнаності).

Тестування на проникнення (Penetration Testing/Pen-test) (Оцінка SysSP).

Це практична перевірка ефективності “технічних” політик.

1. Планування. Команда “етичних хакерів” (Red Team) отримує чітку мету, яка імітує реальну загрозу. Наприклад, “Ваша точка входу – ноутбук розробника. Ваша мета отримати доступ до бази даних клієнтів на фінансовому сервері”.

2. Виконання атаки. Тестери намагаються обійти технічні контролі. Вони не читають політики – вони намагаються їх зламати. Приклад: Політика SysSP (політика сегментації мережі) каже: “Мережа розробників (VLAN 10) не повинна мати прямого доступу до мережі фінансів (VLAN 20)”. Пен-тестер, перебуваючи у VLAN 10, намагається просканувати VLAN 20, шукає неправильні налаштування фаєрволу (Configuration Rules) або слабкі ACLs, щоб “перестрибнути” між мережами.

3. Звіт та Оцінка. Звіт показує не “невідповідність” (як в аудиті), а “шляхи атаки” (Attack Path). Приклад: “Ми успішно отримали доступ до сервера 'SRV-FIN-01'. Ваша SysSP (політика сегментації) є неефективною, оскільки правило фаєрволу №47 дозволяє трафік з 10.1.1.5 (ноутбук розробника) на 10.2.2.10 (фін. сервер) через порт RDP”.

Саме такий тест міг би виявити провали в LastPass (що інженер має доступ до бекапів) або в MGM (що дзвінок в Help Desk дозволяє скинути MFA).

Практичне тестування є найбільш надійним методом оцінки реальної ефективності політик. Воно перевіряє, чи витримають ваші ISSP (поведінкові) та SysSP (технічні) політики контакт із реальним, вмотивованим зловмисником.

Аналіз інцидентів – це метод оцінки, який проводиться після того, як інцидент безпеки вже стався (наприклад, злам, витік даних, атака ransomware).

Його мета – не просто “залатати дірку”, а провести глибоке розслідування першопричин (Root Cause Analysis – RCA), щоб точно зрозуміти, яка саме політика, процедура або контроль не спрацювали, і чому. Як можна побачити в аналізі звітів DBIR та ДЦКЗ кожен інцидент – це, по суті, доказ того, що одна або декілька політик (або їхнє технічне впровадження) провалилися.

Цей метод є невід’ємною частиною будь-якої сучасної системи управління безпекою.

– NIST CSF 2.0. Цей процес вбудований у функції RESPOND (RS) (Реагування) та IDENTIFY (ID) (Ідентифікація). Зокрема, підкатегорія RS.AN (Incident Analysis) передбачає аналіз інциденту, а ID.IM (Improvement) — використання отриманих знань для вдосконалення, що включає і оновлення політик.

– ISO 27001. Стандарт вимагає процесу “управління інцидентами” та “постійного вдосконалення”. Аналіз того, чому інцидент стався, є ключем до вдосконалення політик.

Етапи аналізу інциденту. Процес починається в момент, коли інцидент оголошено завершеним.

1. Збір даних. Команда реагування (CERT/SOC) збирає всі артефакти, пов’язані з інцидентом:
   – Логи фаєрволів, серверів, EDR.
   – Копії фішингових листів.
   – Інтерв’ю зі співробітниками, які були залучені.
2. Аналіз першопричин (RCA). Команда ставить питання “Чому?” п’ять разів (метод “5 Whys” [41, 42]), щоб дістатися від симптому до причини. Приклад: “Чому стався злам? -> Бо хакер отримав доступ. -> Чому він отримав доступ? -> Бо йому надали облікові дані. -> Чому йому надали дані? -> Бо співробітник Help Desk скинув пароль. -> Чому він скинув пароль? -> Бо він не зміг належним чином верифікувати особу. -> Чому? -> Бо у нас немає чіткої, обов'язкової політики верифікації (ISSP)”.

3. Звіт та Оцінка. Звіт про інцидент повинен чітко вказати, яка саме політика провалилася і чому.

Приклад 1 (Кейс MGM)

– Інцидент. Атака через соціальну інженерію.

– Оцінка. ISSP – а саме, “Політика верифікації особистості в Help Desk” – визнана неефективною (або відсутньою). Її потрібно негайно розробити та впровадити.

Приклад 2 (Кейс LastPass)

– Інцидент. Компрометація інженера та крадіжка бекапів.

– Оцінка. SysSP – а саме, “Політика шифрування даних у стані спокою” та “Політика контролю доступу” – визнані неефективними. Вони існували, але були порушені (незашифровані метадані, вбудовані паролі).

Аналіз інцидентів – це найбільш правдивий і жорстокий метод оцінки. Він не дає “приблизних” результатів (як симуляція фішингу) і не перевіряє “папірці” (як аудит). Він показує реальний, доконаний факт: “Ця політика не спрацювала, і ось збитки”. Це найпотужніший драйвер для реальних змін у політиках безпеки.

Таким чином, жоден з методів не є вичерпним. Ефективна оцінка вимагає комбінованого підходу: регулярний аудит (для перевірки формальної відповідності), оцінка зрілості (для стратегічного розуміння процесів) та практичне тестування (для проактивної перевірки стійкості). Якщо ж ці методи не спрацювали, аналіз інцидентів стає останнім, реактивним інструментом оцінки, який надає найцінніші уроки для вдосконалення

2.4 Проблеми інтеграції етичних, правових і технічних аспектів у політики кібербезпеки

Попередній аналіз доводить, що найбільша проблема полягає не у відсутності технологій, не у відсутності законів і не у відсутності методів оцінки. Головна проблема полягає у “проблемі інтеграції” – відсутності єдиного підходу, який би гармонізував технічні, правові та етичні вимоги.

На практиці ці три аспекти часто розробляються у “силосах”: IT-відділ пише технічні політики, юридичний – правові, а HR – етичні. Це призводить до фундаментальних конфліктів, які політики неефективними, як показано нижче.

Конфлікт А. Технічний (“Можемо”) проти Правового (“Не можна”).

Перший конфлікт виникає між технічними можливостями та юридичними обмеження.

Технічний аспект. Сучасні SysSP дають повну можливість контролю. Системи DLP, EDR та налізу пошти дозволяють IT-відділу бачити, аналізувати та блокувати будь-який трафік співробітників для захисту від вірусів та витоків даних.

Правовий аспект. Однак, Закон України “Про захист персональних даних” (як проаналізовано в табл.1.3) прямо забороняє такий тотальний контроль. Принцип “Мети” (Ст. 6) вимагає, щоб була чітка, законна мета, а Принцип “Згоди” (Ст. 6, 11) забороняє обробку (якою є і моніторинг) без згоди суб’єкта.

Виникає пряма колізія. IT-відділ не може реалізувати технічно ефективну політику SysSP, оскільки вона незаконна без інтеграції з правовими вимогами ISSP (отримання згоди).

Конфлікт Б. Правовий (“Можна, якщо…”) проти Етичного (“Чи варто?”).

Другий конфлікт виникає, коли правова проблема нібито вирішена, але етична – ні.

Правовий аспект. Організація може вирішити Конфлікт А, змусивши всіх співробітників при прийомі на роботу підписати ISSP “Політика допустимого використання”, де є пункт про “добровільну згоду” на моніторинг. Тепер моніторинг стає законним.

Етичний аспект. Проте, як було розглянуто в підпункті 1.4, це створює етичну дилему. Чи є “згода”, отримана під загрозою звільнення, справді “добровільною”? Такий підхід створює “культуру недовіри”, розмиває межі особистого життя і порушує етичний баланс між безпекою та приватністю.

Політика, яка є технічно можливою та юридично захищеною, може бути етично провальною, що призводить до плинності кадрів та зловживань.

Конфлікт В. Організаційний (Політика існує, але не працює).

Третя, і найпоширеніша, проблема інтеграції – це провал комунікацій та впровадження.

Організація може мати ідеально збалансовану політику, але вона залишається “на папері” (як було визначено в 2.3). Аналіз звітів DBIR та ДЦКЗ доводить це: DBIR 2025 показує, що 72% співробітників викоритсовують GenAI “поза межами корпоративної політики”, 46% скомпрометованих пристроїв – це BYOD, що використовується “поза межами дозволеної політики”; ДЦКЗ 2024 показує, що фішинг залишається головних вектором атаки, незважаючи на те, що політики забороняють відкривати підозрілі листи.

Політики часто пишуться складною “юридичною” або “технічною” мовою, не інтегруються в реальні робочі процеси і не доносяться до персоналу. Це не проблема змісту політики, а проблема її інтеграції в організаційну культуру.

Таким чином, проведений аналіз виявляє ключову системну проблему: політики часто розробляються у відриві одна від одної, у “силосах” оремих підрозділів. Це призводить до прямих конфліктів:

– Технічні політики суперечать правовим (Закон про ПД);

– Правові політики (ISSP зі згодою) суперечать етичним (баланс довіри та приватності);

– Організаційні політики провалюються, оскільки вони не інтегровані в культуру та не доносяться до персоналу, що доведено статистикою DBIR та ДЦКЗ.

Ці проблеми доводять, що в організаціях відсутній єдиний, інтегрований підхід до життєвого циклу політик. Це обґрунтовує гостру необхідність у розробці методичних підходів (єдиної моделі процесу), яка б вирішувала ці проблеми, інтегруючи технічні, правові та етичні вимоги на кожному етапі.

Висновки до розділу 2

У другому розділі було проведено комплексний аналіз сучасного стану формування та впровадження політик кібербезпеки на міжнародному та вітчизняному рівнях.

Міжнародний досвід, зокрема результати звіту Verizon Data Breach Investigations Report (DBIR) 2025, показав, що більшість кіберінцидентів (понад 60%) мають “людський елемент” як основну причину. Провали поведінкових політик (ISSP), технічних (SysSP) та організаційних (Program Policy) є ключовими чинниками, що призводять до фішингу, зловживань привілеями, неправильних конфігурацій і витоків даних. Це підтверджує, що ефективна кібербезпека починається не з технологій, а з політик і дисципліни їх виконання.

Аналіз українського досвіду, зокрема звіту Державного центру кіберзахисту (ДЦКЗ) за 2024 рік, довів, що вітчизняні організації стикаються з аналогічними проблемами. Головний вектор атак – фішинг та компрометація облікових записів, що свідчить про слабку реалізацію політик поведінкової безпеки. Крім того, велика частина інцидентів зумовлена помилками конфігурацій і недостатньою ефективністю технічних політик SysSP, що перетворює людські помилки на масштабні інциденти.

Дослідження практичних кейсів – атаки на MGM Resorts (2023) та злам LastPass (2022) – продемонстрували, що навіть великі корпорації зазнають катастрофічних наслідків через недостатньо продумані або невиконувані політики. У випадку MGM – це провал поведінкової політики верифікації, у LastPass – провал технічних політик контролю доступу та шифрування.

Розділ також показав, що наявність політики не гарантує її ефективності. Для цього необхідно здійснювати постійні аудити, оцінку зрілості, тестування та аналіз інцидентів. Міжнародні стандарти, такі як ISO/IEC 27001:2023 та NIST CSF 2.0, визначають ці процеси як обов’язкові складові управління інформаційною безпекою.

Окремо було виявлено проблему інтеграції етичних, правових і технічних аспектів. Політики часто створюються окремими підрозділами – юридичними, IT або HR – без узгодження між собою. Це породжує конфлікти: технічні політики суперечать правовим вимогам (наприклад, моніторинг проти закону про персональні дані), а правові – етичним принципам (згода працівників на контроль). Як наслідок, навіть формально коректні політики залишаються неефективними на практиці.

Загалом, проведений аналіз довів, що ефективна система кібербезпеки неможлива без інтегрованого підходу до політик, який поєднує технічні, правові, етичні та організаційні вимоги. Саме це створює передумови для розробки єдиної методичної моделі життєвого циклу політик кібербезпеки, що буде представлена у наступному розділі.

РОЗДІЛ 3

МЕТОДИЧНІ ПІДХОДИ ДО РОЗРОБКИ ПОЛІТИК КІБЕРБЕЗПЕКИ З УРАХУВАННЯМ ЕТИЧНИХ, ПРАВОВИХ ТА ТЕХНІЧНИХ АСПЕКТІВ

Аналіз, проведений у попередньому розділі, засвідчив, що ключовою причиною неефективності політик кібербезпеки є відсутність системного підходу до їх формування. Існуюча практика розробки політик окремими підрозділами створює конфлікти між технічними можливостями, правовими обмеженнями та етичними нормами. Метою цього розділу є розробка комплексних методичних підходів, які дозволять інтегрувати ці три аспекти в єдиний, узгоджений процес. У розділі пропонується нова методика життєвого циклу політик, методика формування вимог та практичні механізми їх технічної реалізації в системах моніторингу подій (SIEM).

3.1 Методика процесу розробки та впровадження політик кібербезпеки в організації

У розділі 2 було доведено, що ключовою причиною провалу політик є не відсутність технологій чи стандартів, а системні проблеми інтеграції. Технічні, правові та етичні аспекти конфліктують, оскільки розробляються у “силосах” окремих підрозділів. Для вирішення цієї проблеми пропонується нова методика (рис. 3.1) процесу розробки та впровадження політик, яка забезпечує узгодженість на всіх етапах життєвого циклу.

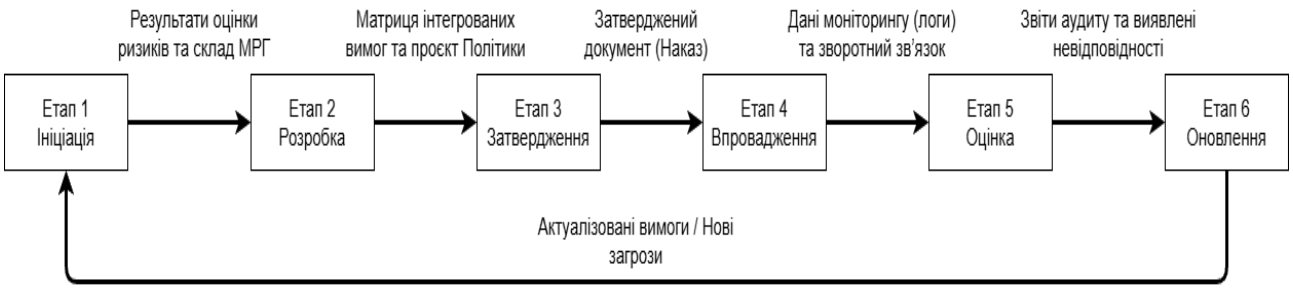


Рис. 3.1. Візуалізація методики

Процес розробки в рамках цієї методики складається з шести послідовних та циклічних етапів:

Етап 1: Ініціація та Формування Робочої Групи.

Це початковий етап, який запускається, коли виникає потреба у новій політиці або перегляді існуючої. Це може бути викликано:

– зовнішніми факторами (наприклад, вийшов новий Закон “Про захист ПД” або GDPR);

– технологічними змінами (впровадження GenAI або BYOD, як можна побачити у DBIR);

– бізнес-потребами (вихід на новий ринок).

На цьому етапі обов’язково формується “Міждисциплінарна робоча група” (МРГ), яка вирішує “проблему силосів”. До неї входять:

– представник IT-безпеки/Кібербезпеки (відповідає за технічні аспекти);

– юрист (відповідає за правові аспекти, відповідність законам);

– представник HR/Менеджменту (відповідає за етичні та організаційні аспекти).

Також, критично важливим є проведення оцінки для обґрунтування необхідності політики. Для цього МРГ повинна використовувати методологію, визначену в стандартах NIST SP 800-39 [43], NIST SP 800-37 [44],NIST SP 800-30 [45], а також враховувати рекомендації міжнародних стандартів ISO/IEC 27005 [46] та ISO 31000 [47].

Етап 2: Розробка (Інтегрований аналіз вимог).

На цьому етапі МРГ спільно розробляє чернетку політики. Це вирішує конфлікти з підпункту 2.4 до їх появи.

– Юрист каже: “Технічно ми можемо моніторити пошту (SysSP), але законно це лише зі згодою (ISSP)” (вирішення Конфлікту А).

– HR каже: “Якщо ми вимагатимемо тотальну згоду, це етично вдарить по довірі. Давайте чітко пропишемо тільки бізнес-цілі моніторингу” (вирішення Конфлікту Б).

– IT каже: “Добре, ми налаштуємо SysSP так, щоб вона технічно не торкалася приватних повідомлень”.

Етап 3: Затвердження (Схвалення Керівництвом).

Готова, вже узгоджена чернетка передається вищому керівництву (наприклад, CISO або CEO) для офіційного затвердження. Це перетворює документ з “проєкту” на “закон організації”.

Етап 4: Впровадження та Комунікація.

Це критичний етап, який вирішує “Конфлікт В” з підпункту 2.4. Він ділитьс на два паралельні процеси:

1. Технічне впровадження: IT-відділ впроваджує SysSP.

2. Організаційне впровадження (Комунікація): HR та юристи доносять ISSP до персоналу. Це не просто розсилка e-mail, а повноцінний процес: тренінги, воркшопи, пояснення чому це важливо, отримання підписів про ознайомлення. Це вирішує проблему з DBIR, де персонал порушує політики, бо не знає про них або не розуміє їх.

Етап 5: Оцінка ефективності.

Як дізнатися, що політика працює? На цьому етапі застосовується комбінований підхід, який бу обґрунтований у підпункті 2.3:

– Регулярний Аудит (для перевірки формальної відповідності);

– Оцінка зрілості (NIST Tiers), яка базується на метриках фреймворку управління COBIT 2019 [48];

– Практичне тестування (симуляції фішингу, Pen-test);

– Аналіз інцидентів (RCA).

Етап 6: Оновлення.

Результати Етапу 5 є вхідними даними для цього етапу. Політика – це “живий документ”. Якщо оцінка виявила проблему, процес повертається на Етап 1. Робоча група знову збирається, і цикл починається спочатку для оновлення політики.

3.2 Формування вимог до політики безпеки (етичні, правові, технічні)

Як було визначено у методиці, найважливішим етапом, що вирішує проблему, є “Етап 2: Розробка”. На цьому етапі МРГ повинна спільно сформувати набір інтегрованих вимог до того, як буде написано перше речення самої політики.

Мета цього етапу – заздалегідь виявити та вирішити конфлікти, які були проаналізовані у підпункті 2.4. Для цього МРГ має послідовно відповісти на низку ключових запитань, які формують вимоги до документа.

1. Формування Етичних вимог.

Першим кроком МРГ на етапі розробки має бути не технічне планування, а етична валідація ідеї. Мета цього блоку – гарантувати, що політика буде не лише ефективною, а й сприйнятою для людей, що мінімізує опір персоналу та ризик внутрішніх загроз.

МГТ повинна сформулювати вимоги, відповідаючи на такі ключові питання:

– **Вимога прозорості та зрозумілості.** Як показав аналіз DBIR та ДЦКЗ, основною причиною інцидентів є помилки людей. Часто це стається тому, що політики написані складною юридичною або технічною мовою, яку зазвичай користувач не розуміє.

Текст політики має бути адаптований під конкретну цільову аудиторію. Сам критерій має відповідати на питання: “Чи розуміє цю вимогу новий співробітник без технічної освіти?”. Етичним принципом є: Співробітник не може нести відповідальність за порушення правил, яких він не розумів.

– **Вимога мінімізації втручання.** Це пряма відповідь на конфлікт “безпека vs. приватність”. МРГ має чітко розмежувати зони контролю, особливо в умовах використання BYOD.

Політика повинна чітко визначити не лише те, що моніториться, але й те, що категорично не моніториться. Наприклад, “Ми моніторимо трафік корпоративної пошти для захисту від вірусів, але ми технічно гарантуємо відсутність доступу до особистих месенджерів на особистому смартфоні співробітника, навіть якщо він підключений до корпоративного Wi-Fi”. Повага до особистого простору підвищує лояльність і зменшує ризик саботажу.

– **Вимога “Справедливої гри”.** Політика не повинна створювати “культуру страху”. Санкції мають бути пропорційними. Вона повинна передбачати диференційовану відповідальність залежно від умислу. Наприклад: Якщо співробітник став жертвою складного фішингу (який важко розпізнати), це має розглядатися як привід додаткового навчання, а не покарання. Якщо ж це свідоме ігнорування правил – це підстава для дисциплінарних дій. Культура безпеки має будуватися на співпраці, а не на покаранні за помилки.

– **Вимога реальної (а не формальної) згоди.** Як було визначено в 2.4, “добровільна згода” під загрозою звільнення є фікцією.

МРГ має забезпечити механізм інформованої згоди, де співробітнику пояснюють мету обмежень. (наприклад, “ми блокуємо USB-порти не тому, що не довіряємо вам, а щоб вірус-вимагач не знищив вашу роботу”. Це перетворює вимогу з “з наказу” на “спільну домовленість”, що є основою етичного підходу.

Результатом роботи над цим блоком є набір етичних обмежень для майбутньої політики.

2. Формування Правових вимог.

Мета цього блоку – перетворити абстрактні норми законів на конкретні обмеження для тексту політики. Юрист у складі МГТ має перевірити кожну ініціативу на відповідність нормативній базі.

МРГ повинна сформулювати вимоги, відповідаючи на такі ключові питання:

– **Вимога законності мети.** Це пряма вимога Ст. 6 Закону Україні “Про захист персональних даних” та принципу GDPR. Політика не може містити розмитих формулювань типу “для покращення безпеки”. Мета будь-якого моніторингу чи обмеження має бути сформульована чітко і конкретно. Замість “Ми можемо переглядати файли співробітників”, політика має казати: “Моніторинг файлової активності здійснюється виключно з метою виявлення та запобігання витоку конфіденційної інформації (DLP) та захисту від шкідливого ПЗ”. Якзо мета не визначена, будь-який зібраний зібраний доказ може бути визнаний судом недійсним.

– **Вимога правової підстави.** Це вирішення проблеми згоди. РГТ має визначити, на якій підставі діє політика. Для кожної дії з даними має бути визначена правова підстава.

Ключове питання: Чи потрібна нам згода співробітника?

Якщо це стосується безпеки мережі, це може бути обґрунтовано “законним інтересом” або “виконання обов’язку володільця”.

Якщо це стосується змісту комунікацій, згода є обов’язком. Політика повинна передбачати механізм отримання цієї згоди.

– **Вимога відповідності секторним нормам.** Якщо організація є об’єктом критичної інфраструктури, політика має враховувати вимоги Закону “Про основні засади кібербезпеки України”. Політика реагування на інциденти (ISSP) повинна містити обов’язкову норму про повідомлення CERT-UA/Держспецзв’язку про інциденти, як того вимагає Ст. 6 Закону.

– **Вимога відповідності стандартам.** Політика має допомагати, а не заважати проходження аудитів. Вимога повинна задати питання: “Чи покриває ця політика вимоги ДСТУ ISO/EIC 27001:2023?”. Для Program Policy МРГ має перевірити, чи є там пункт про “постійне вдосконалення”. Для SysSP – чи реалізовано “принцип найменших привілеїв”.

Результатом цього блоку є юридична верифікація.

3. Формування Технічних вимог.

Після того, як вимога пройшла етичну та юридичну перевірку, вона має пройти технічну валідацію. Мета цього блоку – гарантувати, що політика не залишиться “декларацією про наміри”, а буде технічно здійсненною та контрольованою.

МРГ повинна сформулювати вимоги, відповідаючи на такі ключові питання:

– **Вимога технічної здійсненності.** Це перевірка реальності. Частою юристи або менеджмент пишуть вимоги, які неможливо виконати наявною інфраструктурою. Кожне положення політики має бути прив’язане до конкретного технічного механізму реалізації. Якзо технічного засобу немає, МРГ має або змінити політику (“не рекомендується” замість “заборонено”), або ініціювати закупівлю відповідного ПЗ (що повертає нас до Етапу 1: Ініціація).

– **Вимога примусового виконання.** Це вимога стандарту NIST CSF 2.0 (GV.PO-01) [25]: політика має бути “забезпечена виконанням”. Перевага має надаватися технічному примусу, а не адміністративному. Наприклад: Замість того щоб писати в ISSP: “Користувачі зобов’язані створювати складні паролі”, треба прописати в SysSP налаштування Active Directory, яке технічно не дозволити зберегти пароль простіший за 12 символів.

– **Вимога вимірюваності та аудиту.** Політика, виконання якої неможливо перевірити, є марною. Це вирішує проблему оцінки ефективності. Для кожної політики має бути визначений технічний індикатор (лог, подія, звіт), який підтвердить її виконання або порушення. Наприклад: “Політика:

“Доступ до фінансової системи надається лише з офісу”. Технічна вимога: “Фаєвол та VPN-шлюз повинні вести логи всіх з’єднань із фіксацією IP-адрес. Має бути налаштований алерт в SIEM-систему при спробі входу з невідомого IP””. Це забезпечує можливість проведення Аудиту та Аналізу інцидентів на пізніших етапах.

– **Інтеграція з “найкращими практиками”.** МРГ не повинна вигадувати велосипед. Технічні вимоги мають базуватися на стандартах. Кожен пункт політики моє посилатися на відповідний контроль з ISO 27001 (Додаток А) або NIST SP 800-12.

Результатом роботи МРГ на цьому етапі є не сама політика, а проміжний документ – “Матриця Інтегрованих Вимог”. Ця матриця гарантує (табл. 3.1), що будь-яка вимога, яка потрапить у фінальний текст політики, є збалансованою:

1. Етично прийнятною. Пройшла валідацію HR (не руйнує довіру, прозора).

2. Юридично коректною. Пройшла валідацію юриста (відповідаю Закону про ПД).

3. Технічно можливою. Пройшла валідацію IT (є інструменти для її виконання та контролю).

Такий підхід вирішує “проблеми інтеграції” ще до написання самої політики, що є головною метою запропонованої моделі.

Таблиця 3.1

Матриця Інтегрованих Вимог до політики кібербезпеки

Тип вимог	**Критерій (Вимога)**	**Ключове питання для перевірки**
Етичні	Прозорість та зрозумілість	Чи написаний текст мовою, зрозумілою цільовій аудиторії (без зайвого “юридизму” та “техніцизму”)?
	Мінімізація втручання	Чи чітко визначено межі приватності (що не моніториться, напр., особисті месенджери)?
	Справедливість (“Fair Play”)	Чи передбачена диференційована відповідальність (навчання за помилку vs покарання за умисел)?
	Реальна згода	Чи пояснює політика мету обмежень так, щоб згода співробітника була справді інформованою, а не формальною?
Правові	Законність мети	Чи чітко сформульована конкретна, законна мета обробки даних (згідно зі ст. 6 Закону “Про захист ПД”)?
	Правова підстава	Чи визначено правову підставу (згода, законний інтерес, виконання обов'язку) для кожної дії?
	Секторна відповідність	Чи враховано вимоги до об'єктів критичної інфраструктури (напр., обов'язкове звітування про інциденти)?
	Відповідність стандартам	Чи покриває політика вимоги міжнародних стандартів (ДСТУ ISO 27001, NIST, GDPR)?
Технічні	Технічна здійсненність	Чи існує в організації інструмент (DLP, EDR, Firewall) для реалізації цієї вимоги?
	Примусове виконання	Чи можна забезпечити виконання вимоги технічно, а не покладатися лише на дисципліну людей?
	Вимірюваність (Аудит)	Чи генерує система логи/звіти, які дозволять перевірити виконання цієї вимоги під час аудиту?
	Інтеграція з практиками	Чи базується технічна вимога на визнаних каталогах контролів (NIST SP 800-53, ISO Annex A)?

3.3 Інтеграція технічних методів захисту (ідентифікація, контроль доступу, аудит, реагування на інциденти) у політики безпеки

Після формування інтегрованих вимог на Етапі 2, наступним кроком у запропонованій методиці є їх технічна реалізація (Етап 4). Політика залишається декларативною, доки не буде забезпечена механізмами примусового виконання. Метою цього підрозділу є розробка методики інтеграції ключових технічних методів захисту – ідентифікації, контролю доступу, аудиту та реагування на інциденти – безпосередньо у структуру та правила політик. Буде розглянуто, як перетворити текстові вимоги на налаштування конкретних систем захисту. За основу взято родини контролів, визначені у NIST SP 800-12 Rev. 1 [5] та деталізовані у каталозі контролів NIST SP 800-53 Rev. 5 [49], а також вимоги стандарту ISO/IEC 27001.

1. Інтеграція методів Ідентифікації та Автентифікації.

Цей блок є першою лінією захисту. Як показав аналіз у Розділі 2, компрометація облікових записів є одним з найпоширеніших векторів атак. Тому вимоги “Поведінкової політики” щодо паролів та доступу мають бути жорстко закріплені в “Технічній політиці”.

Трансформація вимоги в налаштування:

Замість покладання на дисципліну користувачів (наприклад, просте прохання “створювати складні паролі”), МРГ повинна ініціювати впровадження технічних контролів, які унеможливлюють створення слабких паролів.

У середовищі Windows це реалізується через Об’єкти групової політики (Group Policy Objects – GPO). Як показано на рис 1.3 (Локальна політика безпеки), адміністратор повинен налаштувати параметри у розділі “Account Policies – > Password Policy”:

– Minimum password length (Мінімальна довжина): Встановити значення 12 або більше символів (відповідно до сучасних рекомендацій NIST).

– Password must meet complexity requirements: Встановити у значення Enabled (Включено).

– Enforce password history: Встановити значення (наприклад, 24), щоб запобігти повторному використання старих паролів.

Посилення через Багатофакторну Автентифікацію (MFA):

Враховуючи неефективність людського фактору проти фішингу, політика ISSP повинна містити вимогу: “Доступ до критичних систем ззовні дозволено лише з використанням MFA”.

Це вимагає налаштування SysSP на рівні служб ідентифікації (наприклад, Azure AD або Okta). Система має бути сконфігурована так, щоб технічно відхиляти будь-яку спробу входу без другого фактора, незалежно від складності пароля. Це забезпечує виконання контролю ISO/IEC 27001 A.5.17 “Authentication information” та відповідає рекомендаціям NIST SP 800-12 (розд. 10.7 “Identification and Authentication”) та спеціалізованого стандарту NIST SP 800-63-4 “Digital Identity Guidelines” [50].

Таким чином, політика перетворюється з “правил поведінки” на “правило конфігурації”, яке діє автоматично.

2. Інтеграція методів Контролю Доступу (Access Control).

Цей блок реалізує один із фундаментальних принципів безпеки – “Принцип найменших привілеїв”. Як показав аналіз інциденту LastPass, надання надмірних прав доступу (наприклад, доступ інженера до бекапів) може призвести до катастрофічних наслідків.

Трансформація вимоги в налаштування:

Політика SysSP повинна визначати матрицю доступу (хто до чого має доступ), а технічні засоби – автоматично ї забезпечувати. Підручник Уітмена та Метторда та стандарт NIST SP 800-12 виділяють два основні механізми такої реалізації:

На рівні файловій системи (Списки контрою доступу – ACLs). Списки ACLs (Access Control Lists) дозволяють налаштувати права доступу з гранулярністю до окремого файлу. Адміністратори налаштовую дозволи (Read, Write, Execute, Modify) для конкретних груп користувачів.

Windows: Як показано на Рис. 1.4, для папки “Project X” група “Developers” може мати права Modify, тоді як група “Sales” – лише Read або взагалі Deny.

Linux: У цих системах це реалізується через команди chmod/setfacl, які визначають права власника (u), групи (g) та інших (o).

Окрім налаштування прав доступу, критично важливим є загальне зміцнення конфігурації операційної системи. Для визначення безпечних параметрів (наприклад, відключення невикористовуваних сервісів, налаштування політик аудиту) рекомендується використовувати галузевий стандарт CIS Benchmarks [51], який надає покрокові інструкції для безпечного налаштування Windows, Linux та хмарних платформ.

На рівні мережі (Правила конфігурації). Це інструкції для мережевих пристроїв (фаєрволів, маршрутизаторів), які регулюють потік даних між сегментами мережі.

Створення правил фільтрації трафіку на основі IP-адрес, портів та протоколів. Наочним прикладом є набір правил для фаєрволу Palo Alto. Наприклад, правило №16 BitTorrent-Deny технічно блокує використання піринговых мереж, автоматично відкидаючи (Dorp) пакети цього додатку. Це технічне виконання вимоги ISSP про заборону неліцензійного ПЗ.

Інтеграція з ідентифікацією. Сучасний підхід вимагає інтеграції ACLs з системою ідентифікації. Політика має вимагати, щоб доступ надався не конкретним користувачам, а ролям/групам. Це значно спрощує управління доступом при звільненні співробітника, оскільки достатньо видалити його з групи в Active Directory, щоб автоматично відкладати всі права. Такий підхід до сегментації та мінімізації прав є кроком до впровадження архітектури “нульової довіри” (Zero Trust Architecture), принцип якої викладені у стандарті NIST SP 800-207 [52]. Згідно з цим стандартом, політика SysSP повинна виходити з припущення, що мережа вже скомпрометована, і вимагати перевірки кожного запиту на доступ.

3. Інтеграція методів Аудиту та Підзвітності.

Цей блок технічно реалізує вимогу “вимірюваності”, яку було сформулювано на Етапі 2. Політика повинна забезпечувати фіксацію дій користувачів та систем для подальшого аналізу

Трансформація вимоги в налаштування:

Політика вищого рівня повинна містити вимогу: “Всі критичні події в інформаційній системі повинні реєструватися та зберігатися”. SysSP транформує цю вимогу в конкретні технічні інструкції щодо того, які саме події фіксувати і як довго їх зберігати.

Технічна реалізація на рівні операційних систем. У найбільшому поширеному корпоративному середовищі інтеграція політики аудиту здійснюється через налаштування Local Security Policy (або через Group Policy для домену).

Як наочно демонструє Рис. 1.6, адміністратор повинен перейти у гілку “Security Setting –> Local Policies – > Audit Policy” і перевести відповідні політики в режим “Enabled” для подій “Success” та/або “Failure”.

Ключові параметри, які має диктувати SysSP:

Audit account login events (Аудит подій входу). Він фіксує кожну спробу входу користувача в систему, що дозволяє виявити атаки з перебором паролів (Brute-force) – сотні подій “Failure” за короткий час, або несанкціонований вхід у нічний час.

Audit object access (Аудит доступу до об’єктів). Фіксує хто відкривав, змінював, видаляв або копіював конкретні файли чи папки. Він дозволяє фіксувати порушення, якщо ISSP забороняє доступ до бази клієнтів.

Audit privilege use (Аудит використання привілеїв). Він фіксує випадки, коли користувач застосовує права адміністратора. Це головний інструмент протидії загрозі “Зловживання привілеями”.

Audit policy change (Аудит зміни політик). Фіксує спроби змінити самі налаштування аудиту, щоб зловмисник не міг “вимкнути сліди” перед вчиненням злочину.

Централізація та захист логів. Просте включення аудиту на локальному комп’ютері є недостатнім, оскільки зловмисник, отримавши повний доступ, може очистити журнал подій (Event Viewer).

Тому сучасна SysSP повинна містити вимогу централізації логів.

Технічне правило: “Налаштувати автоматичну пересилку журналів подій типу Security та System з усіх критичних хостів на захищений сервер логування або в систему SIEM”.

Перевага: Навіть якщо зловмисник знищіть дані на зламаному сервері, копія логів залишається в SIEM, що дозволить провести розслідування.

Відповідність стандартам. Така глибока інтеграція методів аудиту забезпечує виконання:

Контролю ISO/IEC 27001 A.8.15 “Logging”, який вимагає, щоб логи створювалися, зберігалися та регулярно переглядалися [20]. Практичні рекомендації щодо реалізації цього контролю наведені у стандарті ISO/IEC 27002:2022 (A.8.15) [53], що і було враховано при формулюванні вимоги про централізацію логів у SIEM.

Вимог родини контролів AU (Audit and Accountability) зі стандарту NIST SP 800-12 Rev.1 (Розд. 10.3).

4. Інтеграція методів Реагування на інциденти.

Останнім, але критично важливим елементом є інтеграція політик реагування безпосередньо в інфраструктуру. Метою є мінімізація часу реакції та автоматизація захисних дій, що є вимогою у сучасної парадигми NIST CSF 2.0 (Функція RESPOND).

Трансформація вимоги в налаштуваннях:

Incident Response Policy зазвичай описує алгоритм дій для персоналу (наприклад, повідомити CISO, вимкнути сервер). Проте, в умовах швидкоплинних атак, людська реакція є занадто повільною. Тому SysSP повинна містити правила для автоматизації цих дій.

Сучасна технічна реалізація здійснюється через системи EDR (Endpoint Detection and Responses) та SOAR (Security Orchestration, Automation and Response).

Приклад: Політика вимагає “наявної ізоляції скомпрометованих хостів”. Технічно це реалізується правилом EDR-консолі:

Умова: Виявлено процес, що шифрує файли.

Дія: “Isolate Host” (блокувати весь мережевий трафік, крім з’єднання з сервером управління).

Це технічка реалізація стратегії “Стримування” (Containment), яка є критичною частиною реагування згідно з NIST SP 800-12 (розд. 10.9 “Incident Response”). Важливість автоматизації цього етапу підкреслюється у новітньому керівництві NIST SP 800-61 Rev. 3 [54], яке розглядає реагування на інциденти як невід'ємну частину управління ризиками кібербезпеки. Якби така технічна політика була активною в MGM Resorts, вона могла б автоматично локалізувати атаку на ранній стадії, запобігши шифруванню тисяч серверів.

Таким чином, інтеграція технічних методів перетворює політику з паперового документа на набір активних правил, які діють автоматично і постійно. Це забезпечує виконання принципу “Security by Design”, де дотримання політики гарантує самою архітектурною системи, а не лише покладанням на дисципліну користувачів.

Для наочної ілюстрації запропонованого підходу, узагальнений приклад трансформації абстрактних вимог політик у конкретні технічні налаштування SysSP та інструменти реалізації наведено в таблиці 3.2.

Таблиця 3.2

Приклад трансформації вимог політики у технічні налаштування

Вимога політики	**Технічний метод**	**Інструмент реалізації**
Використовувати надійні паролі	Password Policy: Min length = 12	Active Directory (GPO)
Заборонити несанкціонований доступ	Access Control List: Group ‘HR’ = Read Only	File System ACLs
Блокувати торент-трафік	Firewall Rule: Drop ‘BitTorrent’ App	Plato Alto Firewall
Фіксувати спроби злому	Audit Policy: Logon Failure – Enabled	OS Audit/SIEM
Зупиняти віруси-шифрувальники	Response Rule: Isolate Host on Detection	EDR/Antivirus

3.4 Рекомендації щодо створення та підтримки комплексних політик кібербезпеки

Розроблена у попередніх підрозділах методика та механізм інтеграції створюють фундамент для ефективної системи політик. Однак, для забезпечення довгострокової життєздатності цієї системи, організації необхідно дотримуватися низки стратегічних рекомендацій, що базується га кращих світових практиків.

Рекомендація 1. Впровадження модульної архітектури політик.

Фундаментально рекомендацією щодо архітектури системи є перехід від створення монолітних документів до модульної структури. Як зазначається у фаховій літературі, спроба охопити всі аспекти безпеки в єдиному документі робить його громіздким та складним для оновлення. Натомість, доцільно

створювати набір окремих, незалежних документів (модулів) для кожного питання, таких як окрема політика паролів, політика віддаленого доступу чи політика класифікації даних. Такий підхід дозволяє оперативно оновлювати один модуль при зміні технології чи бізнес процесів без необхідності перегляду та перезатвердження всього масиву документації.

Рекомендація 2. Ієрархічне розмежування вимог та інструкцій.

Критично важливим є чітке розмежування рівнів документації відповідно до ієрархічної моделі, розглянутої у першому розділі. Політика повинна відповідати на питання “що” і “чому”, визначаючи стратегічні цілі та вимоги, тоді як процедури мають описувати “як” це реалізувати технічно. Змішування цих понять призводить до швидкого застарівання політик, оскільки технологічні інструкції замінюються значно частіше за принципи безпеки. Тому технічні деталі налаштування доцільно виносити в окремі процедурні документи, залишаючи в самій політиці лише посилання на них.

Рекомендація 3. Формалізація управління винятками.

Для уникнення практики ігнорування правил та виникнення “тіньового IT”, політика повинна передбачити формалізований механізм управління винятками. Жодна політика не здатна покрити сто відсотків бізнес-ситуацій, тому організація має запропонувати процедуру прийняття ризику, яка дозволяє легально відступити від вимог політики за умови офіційного затвердження та на визначений термін. Це переводить порушення з неконтрольованої площини в легальне, кероване поле.

Рекомендація 4. Забезпечення видимості та активна комунікація.

Окрему увагу сліж приділити забезпеченню видимості політик. Як показує статистика інцидентів, значна частина порушень стається через необізнаність персоналу. Стандарт NIST SP 800-12 наголошує, що політика повинна бути “видимою”. Публікація документа на внутрішньому порталі є недостатньою; необхідно впровадити активні методи комунікації, такі як регулярні тренінги, нагадування при вході в систему та обов’язкове отримання підтвердження від співробітників про ознайомлення.

Рекомендація 5. Циклічний перегляд та принцип “Sunset Clause”.

Нарешті, для підтримання актуальності системи безпеки критично важливим є впровадження процедури регулярного перегляду. Політика має розглядатися як “живий документ”. Рекомендація встановити графік обов’язкового перегляду, наприклад, щорічно або після значних змін в інфраструктурі чи інцидентів. Ефективною практикою є застосування принципу “sunset clause”, коли політика автоматично втрачає чинність, якщо вона не була перезатверджена до певної дати, що змушує керівництво регулярно повертатися до питань безпеки.

Таблиця 3.3 підсумує рекомендації.

Таблиця 3.3

Стратегічні рекомендації щодо управління політиками

Проблема	**Рекомендація**	**Очікуваний результат**
Політика є занадто великою та складною для оновлення	Впровадження модульної архітектури	Гнучкість: оновлення окремого модуля не вимагає перегляду всієї системи
Політика швидко застаріває через зміну технологій	Ієрархічне розмежування	Довговічність: принципи залишаються стабільними, змінюються лише інструкції
Виникнення “тіньового IT” та ігнорування правил	Формалізація управління винятками	Контроль: переведення порушень у легальне поле з прийняттям ризиків
Необізнаність персоналу	Забезпечення видимості та комунікація	Культура: перетворення політики з документа на частину щоденної роботи
Накопичення неактуальних документів	Принцип “Sunset Clause”	Актуальність: автоматичне скасування застарілих норм примушує до регулярного перегляду

Впровадження запропонованих рекомендацій дозволяє трансформувати дозволяє трансформувати набір розрізнених документів у цілісну, гнучку та життєздатну систему управління безпекою. Така система здатна адаптуватися до змін у ландшафті загроз та бізнес-середовищі, не втрачаючи своєї актуальності.

Для практичної апробації запропонованої у Розділі 3 моделі, методики формування вимог та технічної інтеграції, у наступному підрозділі буде розроблено пілотний проект – шаблон “Політики допустимого використання”, який втілює всі вищезазначені принципи на практиці.

3.5 Приклад (пілотний проєкт) розробки політики кібербезпеки для умовної або реальної організації

З метою практичної апробації та верифікації ефективності методичних підходів, запропонованих у підрозділах 3.1 – 3.4, у цьому підрозділі здійснюється розробка пілотного проєкту політики кібербезпеки.

Як засвідчив аналіз у Розділі 2, найбільші ризики для сучасних організацій пов’язані з “людським фактором” та відсутністю чітких правил поведінки персоналу в цифровому середовищі. Тому для демонстрації роботи запропонованої інтегрованої моделі було обрано розробку “Політики допустимого використання” (Acceptable Use Policy – AUP).

Вибір саме цього типу політики (ISSP) зумовлений тим, що він є найбільш показовим для цілей даного дослідження, оскільки вимагає одночасного вирішення конфліктів у трьох площинах:

1. Етичний: Забезпечення балансу між необхідністю моніторингу та правом співробітників на приватність.
2. Правовий: Відповідність вимогам GDPR та законодавства України щодо захисту персональних даних.

3. Технічний: Інтеграція вимог політики з сучасними засобами контролю.

Розробка здійснюється на прикладі умовної організації, профіль якої змодельовано на основі типових характеристик та проблем українського IT-сектору в умовах гібридної роботи.

Загальна характеристика об'єкта дослідження.

ТОВ "UkrSec" – це українська продуктова IT-компанія середнього розміру, що спеціалізуєтеся на розробці SaaS-рішень для фінансового сектору.

Штат: 150 співробітників. Структура включає департамент розробки, відділ QA, команду DevOps/SecOps (3 особи), відділ продажів та маркетингу, HR-департамент, юридичний відділ та бухгалтерію.

Режим роботи: Компанія працює за моделлю "Remote-First". Головний офіс знаходиться в Києві, але 80% персоналу працюють віддалено, причому близько 20% співробітників знаходиться за кордоном (в країнах ЄС) через військові дії.

Бізнес-контекст: Компанія перебуває на етапі активного масштабування та виходу на ринок Європейського Союзу, що вимагає підтвердження високого рівня зрілості процесів безпеки.

Діяльність компанії підпадає під кількох сурових регуляторних режимів:

Закон України "Про захист персональних даних": Компанія є володільцем баз персональних даних українських співробітників та клієнтів.

GDPR: Оскільки компанія надає послуги клієнтам з ЄС та моніторить поведінку своїх співробітників, що перебувають в Європі, вона зобов'язана дотримуватися вимог GDPR, включати принципи мінімізації даних та прозорості.

Вимоги клієнтів: Ключові замовники (європейські банки) вимагають від "UkrSec" наявності сертифікації за стандартом ISO/IEC 27001 до кінця поточного року.

Інфраструктура компанії є гібридною та децентралізованою, що ускладнює централізований контроль. Для забезпечення захисту у такому

середовищі використовується підхід, що відповідає матриці контролів хмарної безпеки Cloud Controls Matrix v4.0 [55].

Хмарні середовища: Продуктивні сервіси та середовища розробки розгорнуті в хмарах AWS та Microsoft Azure.

Корпоративні сервіси: Використовується Google Workspace (пошта, документи), Slack (корпоративний месенджер), Jira/Confluence (управління задачами) та GitLab (репозиторій коду).

Обладнання та BYOD: Компанія надає корпоративні ноутбуки лише розробникам. Решта персоналу використовують власні пристрої для доступу до корпоративних ресурсів, що створює значні ризики витоку.

Аналіз поточної проблематики.

Попередній аудит (відповідно до методології п. 2.3) виявив, що існуюча система політик знаходить на рівні зрілості **Tier 1** за NIST CSF 2.0. Основні виявлені проблеми корелюють з актуальними векторами атак OWASP Top 10 [56] та включають:

Некероване використання ШІ: Виявлено випадки завантаження розробниками фрагментів пропрієтарного коду в публічні моделі для оптимізації, що є прямим витоком інтелектуальної власності. Чинні політики це ніяк не регулюють.

Ризики соціальної інженерії: Останні симуляції фішингу показали високий рівень вразливості відділу бухгалтерії (25% натискань на посилання), що свідчить про неефективність поточної політики обізнаності.

Конфлікт приватності та безпеки: Співробітники висловлюють незадоволення впровадженням агентів моніторингу на особистих ноутбуках, вважаючи це порушення приватності. Відсутня чітка угода про розмежування особистих та робочих даних.

Застарілість документації: Існуюча “Політика інформаційної безпеки” датована 2019 роком, не враховує віддалену роботу і є суто формальним документом, який нові співробітники підписують, не читаючи.

Для вирішення цих проблем необхідно розробити нову “Політику допустимого використання”, яка б стала основним документом для користувачів, інтегруючи правові вимоги GDPR, технічні реалії хмарної інфрмаструктури та етичні норми гібридної роботи.

Розробка політики допустимого використання (AUP).

На основі проведеного аналізу та сформованих у п. 3.2 вимог, було розроблено текст “Політики допустимого використання” (AUP). Документ структуровано за модульним принципом та включає чіткі розділи щодо мети, сфери застосування, етичних гарантій та відповідальності.

Ключові особливості розробленого документу:

– Правова відповідність. Текст містить чітке формулювання мети обробки даних (відповідно до ст. 6 Закону “Про захист персональних даних”).

– Етичний баланс. Чітко розмежовано зони моніторингу (робочий трафік vs. особисті месенджери), що відповідає професійним стандартам, зокрема Кодексу етики ACM [57], та вирішує етичний конфлікт приватності.

– Технічна інтеграція. Вимоги сформульовані так, щоб їх виконання забезпечувалося автоматизованими засобами (MLF, DLP), а не лише дисципліною.

Повний текст розробленої Політики з методичними коментарями щодо реалізації вимог наведено у **Додатку А**.

Технічний моніторинг виконання політики засобами IBM QRadar (SIEM).

Політика залишається декларативною, якщо не забезпечено механізм контролю за її дотриманням. Для практичної реалізації контролю розробленої AUP було використано SIEM-систему IBM QRadar Community Edition (CE) [58], розгорнуту на віртуальній машині. Налаштування джерел подій та політик аудиту здійснювалося з урахуванням рекомендацій стандарту NIST SP 800-92 [59].

Метою цього етапу було налаштування правил кореляції для виявлення тактик зловмисників, описаних у базі знань MITRE ATT&K [60]. Було реалізовано наступні сценарії моніторингу:

Сценарій 1. Контроль доступу (Протидія Brute Force)

Вимога Політики (пункт 4) є “Система автоматично блокує спробу підбору паролів”. Для цього було створено право “AUP_Violation_Login_Failure_Spike”.

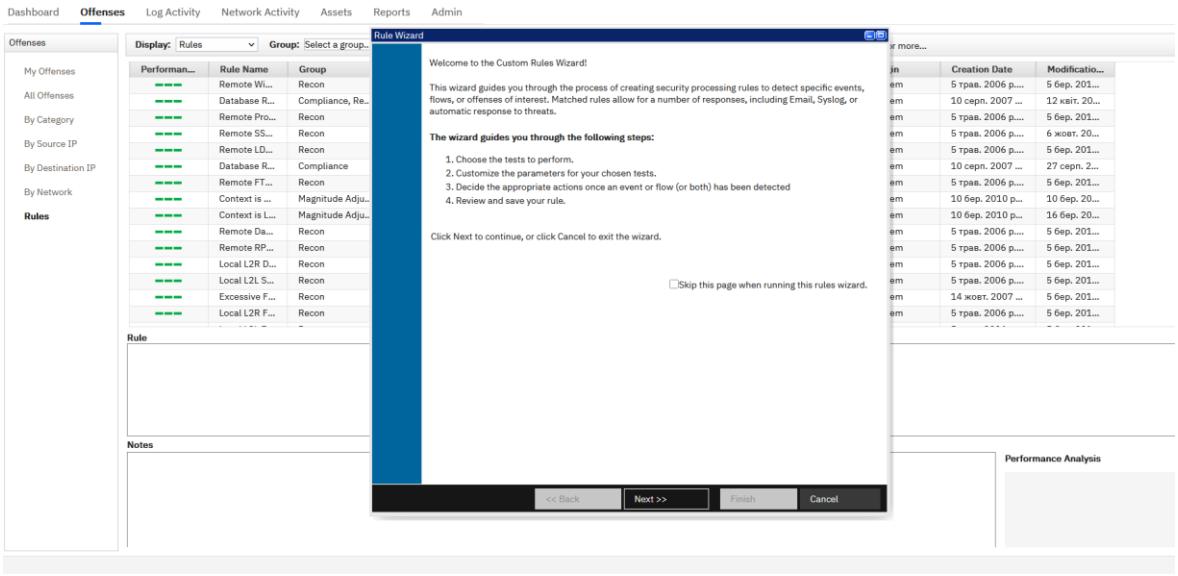


Рис. 3.2. Інтерфейс створення правил кореляції в IBM QRadar

Це правило відстежує події категорії “Authentication Failure” і спрацьовує, якщо з однієї IP-адреси зафіксовано понад 5 помилок входу протягом 5 хвилин. При спрацюванні правила генерується інцидент “Policy Violation: Potential Brute Force”, що дозволяє адміністратору миттєво відреагувати (рис. 3.3).

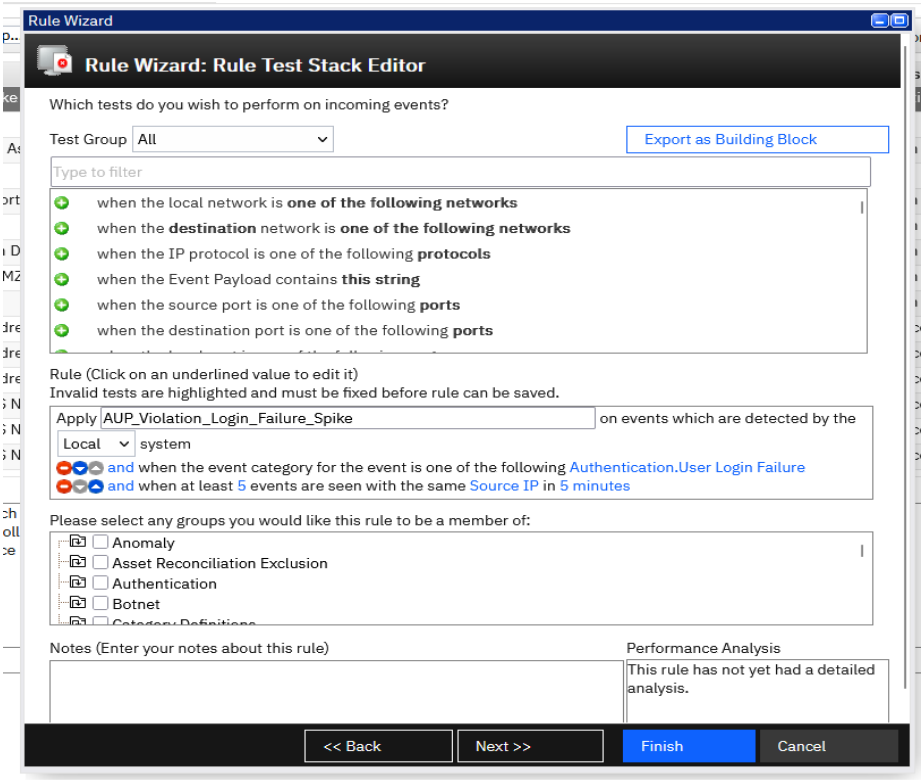


Рис. 3.3. Налаштування правила “AUP_Violation_Login_Failure_Spike”

Сценарій 2. Контроль витоку даних (DLP)

Вимога Політики (пункт 6) є “Заборонено пересилати робочі документі на особисті поштові скриньки”. Для цього треба налаштувати правило “AUP_Violation_Data_Exfiltration_Personal_Mail”, яке аналізує логи поштового шлюзу та виявляє листи з викладеннями, відправлені на публічні домени (gmail.com, ukr.net). В результаті чого буде виконуватися автоматичне виявлення спроб витоку інформації (рис. 3.4).

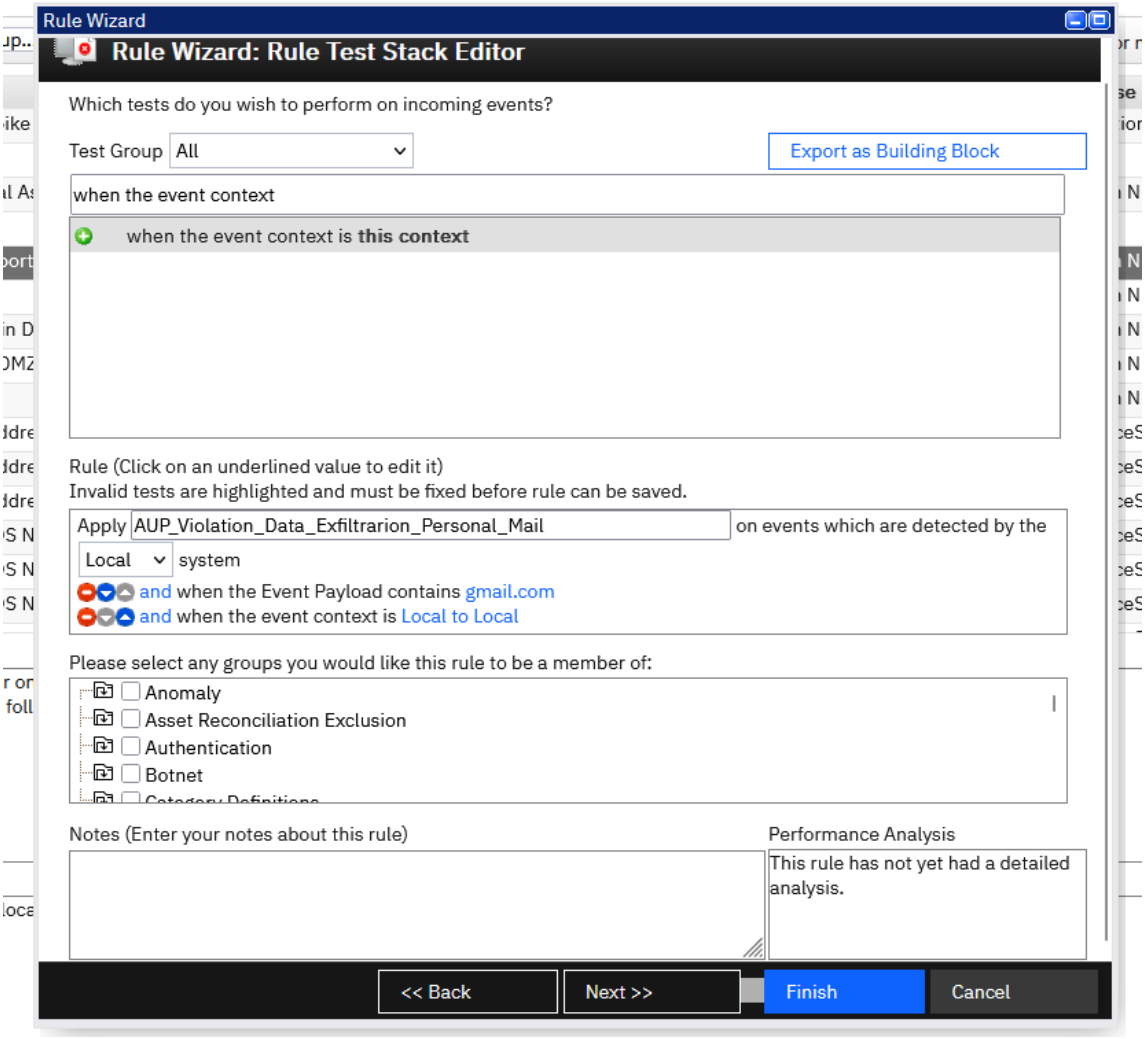


Рис. 3.4. Налаштування правила
“AUP_Violation_Data_Exfiltration_Personal_Mail”

Висновки до розділу 3

У третьому розділі було розроблено комплексний методичний підхід до формування та впровадження політик кібербезпеки, який усуває ключовий недолік традиційних моделей – розрізненість між технічними, правовими та етичними аспектами. Запропонована інтегрована модель життєвого циклу політик усуває “силосний” підхід і забезпечує узгодженість на всіх етапах: від ініціації до регулярного оновлення.

Було запропоновано шестиступеневу модель процесу розробки політик кібербезпеки, що охоплює формування міждисциплінарної робочої групи, інтегрований аналіз вимог, затвердження, впровадження, оцінювання ефективності та періодичне оновлення. Такий підхід перетворює політику з формального документа у живий, динамічний інструмент управління кіберризиками, що відповідає сучасним загрозам і змінам бізнес-середовища.

Особливу увагу було приділено формуванню інтегрованих вимог – етичних, правових та технічних. Розроблена “Матриця інтегрованих вимог” гарантує, що кожне положення політики є:

– етично прийнятним (не порушує довіру та право на приватність);

– юридично обґрунтованим (відповідає вимогам законодавства та стандартів);

– технічно здійсненним (має реальний механізм реалізації та контролю).

Запропоновано методику інтеграції ключових технічних заходів безпеки (ідентифікації, контролю доступу, аудиту та реагування на інциденти) безпосередньо у структуру політик. Це дозволяє перетворити загальні вимоги політики у конкретні конфігураційні рішення (SysSP), реалізовані через сучасні інструменти захисту: GPO, ACL, MFA, EDR, SIEM, SOAR тощо. Таким чином, дотримання політики забезпечується не лише дисципліною персоналу, а й архітектурою самої системи захисту (принцип Security by Design).

Окремим важливим результатом розділу стала розробка стратегічних рекомендацій щодо створення та підтримки політик: перехід до модульної архітектури, ієрархічне розмежування політик і процедур, формалізація управління винятками, посилення комунікації з персоналом та впровадження регулярного перегляду за принципом “sunset clause”. Це забезпечує довгострокову актуальність та адаптивність системи безпеки.

Крім того, запропонована модель була практично апробована на прикладі умовної організації ТОВ “UkrSec” шляхом розробки пілотної “Політики допустимого використання” та реалізовано технічний моніторинг її дотримання

засобами SIEM-системи QRadar. Створені правила кореляції дозволили автоматизувати виявлення порушень, що підтверджує ефективність запропонованого підходу на практиці. Також, даний приклад продемонстрував, яким чином теоретичні положення можуть бути трансформовані у прикладний, реалістичний та юридично обґрунтований документ, що враховує особливості гібридної роботи, використання BYOD, ризики GenAI та вимоги стандартів ISO/IEC 27001 і GDPR.

Таким чином, у третьому розділі було не лише запропоновано теоретичну модель, але й доведено її практичну доцільність та ефективність у сучасних умовах зростаючих кіберзагроз і високих регуляторних вимог. Результати розділу створюють надійну методичну базу для впровадження комплексної системи політик кібербезпеки в реальних організаціях різного масштабу та профілю діяльності.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне наукове-практичне завдання підвищення ефективності систем кібербезпеки організацій шляхом розробки та обґрунтування методичних підходів до формування політик, що забезпечують комплексну інтеграцію етичних, правових та технічних аспектів.

За результатами проведеного дослідження здійснено теоретичне узагальнення та систематизацію понятійного апарату у сфері управління інформаційною безпекою. Визначено, що політика кібербезпеки є фундаментальним управлінським інструментом, який формалізує стратегічні цілі організації та регламентує поведінку суб'єктів. На основі аналізу стандартів NIST SP 800-12 та SP 800-14 удосконалено класифікацію політик за трирівневою ієрархічною моделлю, що включає організаційні, поведінкові та технічні політики. Також встановлено, що нормативно-правова база України та міжнародні стандарти, такі як ISO/IEC 27001 і GDPR, всувають жорсткі вимоги до прозорості, законності мети та підзвітності процесів обробки даних.

Аналіз сучасного стану впровадження політик, проведений на основі міжнародних звітів Verizon DBIR 2025 та національних даних ДЦКЗ 2024, дозволив виявити, що домінуючим фактором інцидентів залишається "людський елемент", зокрема соціальна інженерія, помилки конфігурації та зловживання правами. Це свідчить про низку ефективність існуючих поведінкових політик. На прикладі практичних кейсів, таких як атака на MGM Resorts та злам LastPass, доведено, що критичні засоби захисту впроваджуються ізольовано від процедурних та правових норм, що призводить до системних збоїв.

На основі виявлених проблем розроблено методичні підходи до створення політик кібербезпеки. Зокрема, запропоновано інтегровану циклічну модель процесу розробки, яка передбачає обов'язкове залучення міждисциплінарної робочої групи на етапі ініціації, що дозволяє мінімізувати конфлікти між необхідністю технічного контролю та дотриманням прав

співробітників. Також розроблено методику формування вимог на основі авторської “Матриці інтегрованих вимог”, яка забезпечує попередню валідацію правил за критеріями етичності, законності та технічної реалізованості. Додатково обґрунтовано механізми технічної інтеграції, що дозволяють трансформувати декларативні положення політик у автоматизовані налаштування засобів захисту, забезпечуючи виконання принципу Security by Design.

Здійснено практичну апробацію запропонованих підходів на прикладі умовної організації ТОВ “UkrSec”. Розроблено пілотний проєкт “Політики допустимого використання”, який демонструє практичне вирішення конфлікту між безпекою та приватністю в умовах гібридної моделі роботи та вимог GDPR.

Наукова новизна одержаних результатів полягає в удосконаленні моделі життєвого циклу політик кібербезпеки, яка, на відміну від існуючих лінійних підходів, базується на принципі інтегрованої взаємодії технічних, правових та етичних компонентів на етапі розробки, що дозволяє усунити міждисциплінарні конфлікти та підвищити рівень комплаєнсу. Крім того, набуло подальшого розвитку методичне забезпечення процесу формування вимог до політик шляхом введення “Матриці інтегрованих вимог”, яка систематизує критерії перевірки для забезпечення відповідності NIST CSF 2.0.

Практичне значення одержаних результатів визначається тим, що запропонований алгоритм технічної інтеграції дозволяє організаціям перейти від формального документування до впровадження дієвих автоматизованих механізмів контролю. Водночас розроблений шаблон “Політики допустимого використання” та сформульовані стратегічні рекомендації можуть бути безпосередньо використані українськими підприємствами для побудови систем захисту, адаптованої до сучасних загроз та вимог національного законодавства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України : Аналіт. доп. Київ : Нац. ін-т стратег. дослідж. (НІСД), 2011. 31 с.

2. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В. Бурячок та ін. Київ : ДУТ, 2015. 288 с.

3. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних : підручник. Київ : НВП «Інтерсервіс», 2009. 713 с.

4. Марущак А. І. Інформаційне право України : підручник. Київ : Дакор, 2011. 456 с.

5. Nieles M., Dempsey K., Pillitteri V. Y. An introduction to information security. Gaithersburg, MD : National Institute of Standards and Technology, 2017. URL: https://doi.org/10.6028/nist.sp.800-12r1 (дата звернення: 29.11.2025).

6. Whitman M. E., Mattord H. J. Management of information security : підручник. 6-те вид. Boston, MA : Cengage Learning, 2018. 672 с.

7. Swanson M., Guttman B. Generally accepted principles and practices for securing information technology systems. Gaithersburg, MD : National Institute of Standards and Technology, 1996. URL: https://doi.org/10.6028/NIST.SP.800-14 (дата звернення: 22.10.2025).

8. Cybersecurity policies and standards | SANS institute. SANS Institute. URL: https://www.sans.org/information-security-policy (дата звернення: 24.10.2025).

9. SANS Institute. Program management policy. 2025. URL: https://sansorg.egnyte.com/dl/djhfHVw3fBGq (дата звернення: 24.10.2025).

10. SANS Institute. Email management policy. 2025. URL: https://sansorg.egnyte.com/dl/ghBBLaF8ej (дата звернення: 24.10.2025).

11. SANS Institute. Mobile device management policy. 2025. URL: https://sansorg.egnyte.com/dl/KpQn88OEh1 (дата звернення: 24.10.2025).

12. SANS Institute. Artificial intelligence standard. 2025. URL: https://sansorg.egnyte.com/dl/hHTk98iZYW (дата звернення: 24.10.2025).

13. SANS Institute. Acceptable use standard. 2025. URL: https://sansorg.egnyte.com/dl/3Z3hUcQXEQ (дата звернення: 24.10.2025).

14. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 24.10.2025).

15. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 24.10.2025).

16. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 24.10.2025).

17. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 24.10.2025).

18. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 24.10.2025).

19. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 24.10.2025).

20. Нормативно-правова база у сфері захисту об'єктів критичної інфраструктури України. CSIRT Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації. URL: https://csirt.csi.cip.gov.ua/uk/pages/cio (дата звернення: 24.10.2025).

21. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19.06.2019 № 518 : станом на 20 листоп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 24.10.2025).

22. Деякі питання об'єктів критичної інформаційної інфраструктури : Постанова Каб. Міністрів України від 09.10.2020 № 943 : станом на 18 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text (дата звернення: 24.10.2025).

23. Деякі питання об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 09.10.2020 № 1109 : станом на 13 берез. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text (дата звернення: 24.10.2025).

24. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. системи керування інформаційною безпекою. вимоги (ISO/IEC 27001:2022, IDT). Чинний від 2023-08-22. Вид. офіц. Київ : ДП «УкрНДНЦ», 2023.

25. Nist G. M. The NIST cybersecurity framework 2.0. Gaithersburg, MD : National Institute of Standards and Technology, 2023. URL: https://doi.org/10.6028/nist.cswp.29 (дата звернення: 23.10.2025).

26. Загальний регламент про захист даних (GDPR). GDPR TEXT. URL: https://gdpr-text.com/uk/ (дата звернення: 03.11.2025).

27. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 30.11.2025).

28. Verizon. 2025 data breach investigations report. Verizon, 2025. 117 с. URL: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf (дата звернення: 24.10.2025).

29. IBM. Cost of a data breach report 2024. 2024. 46 с. URL: https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf (дата звернення: 28.10.2025).

30. Microsoft. Microsoft digital defense report 2024. 2024. 113 с. URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20(1).pdf (дата звернення: 26.10.2025).

31. European Union Agency for Cybersecurity (ENISA). ENISA threat landscape 2024. 130 с. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf (дата звернення: 27.10.2025).

32. Center for Internet Security (CIS). CIS critical security controls (CIS controls) v8. 2021. URL: https://www.cisecurity.org/controls/v8 (дата звернення: 24.10.2025).

33. Державна служба спеціального зв'язку та захисту інформації України. Річний звіт Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2024 рік. Держ. центр кіберзах., 2025. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (дата звернення: 25.10.2025).

34. Schrader D. An overview of the MGM cyber attack | netwrix. Data Security that Starts with Identityâ„¢ | Netwrix. URL: https://netwrix.com/en/resources/blog/mgm-cyber-attack/ (дата звернення: 10.11.2025).

35. Gomez F. MGM resorts cyberattack 2025 – lessons, costs & recovery. Inszone Insurance. URL: https://inszoneinsurance.com/blog/cyberattack-mgm-resort-explained (дата звернення: 10.11.2025).

36. Hinojosa G. MGM breach: lessons learned for cybersecurity teams | cobalt. Cobalt: Offensive Security Services. URL: https://www.cobalt.io/blog/lessons-learned-from-the-mgm-breach (дата звернення: 10.11.2025).

37. Breaking the vault: a case study of the 2022 lastpass data breach / J. Gentles та ін. 7 с. (Препринт. Cornell University ; arXiv:2502.04287). URL: https://arxiv.org/abs/2502.04287 (дата звернення: 12.11.2025).

38. Kapko M. LastPass breach timeline: how a monthslong cyberattack unraveled. Cybersecurity Dive. URL: https://www.cybersecuritydive.com/news/lastpass-cyberattack-timeline/643958/ (дата звернення: 12.11.2025).

39. Culafi A. LastPass breach tied to hack of engineer's home computer | TechTarget. Search Security. URL: https://www.techtarget.com/searchsecurity/news/365532032/LastPass-breach-tied-to-hack-of-engineers-home-computer (дата звернення: 12.11.2025).

40. Kan M. LastPass employee could've prevented hack with a software update. pcmag. URL: https://www.pcmag.com/news/lastpass-employee-couldve-prevented-hack-with-a-software-update (дата звернення: 12.11.2025).

41. 39. How to use the 5 Whys method to solve complex problems. IMD business school for management and leadership courses. URL: https://www.imd.org/blog/strategy/the-5-whys-technique/ (дата звернення: 13.11.2025).

42. 5 whys - what is it? | lean enterprise institute. Lean Enterprise Institute. URL: https://www.lean.org/lexicon-terms/5-whys/ (дата звернення: 13.11.2025).

43. Managing information security risk :. Gaithersburg, MD : National Institute of Standards and Technology, 2011. URL: https://doi.org/10.6028/nist.sp.800-39 (дата звернення: 08.12.2025).

44. Risk management framework for information systems and organizations:. Gaithersburg, MD : National Institute of Standards and Technology, 2018. URL: https://doi.org/10.6028/nist.sp.800-37r2 (дата звернення: 08.12.2025).

45. Guide for conducting risk assessments. Gaithersburg, MD : National Institute of Standards and Technology, 2012. URL: https://doi.org/10.6028/nist.sp.800-30r1 (дата звернення: 08.12.2025).

46. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Вид. офіц. Geneva : ISO, 2022. 62 с.

47. ISO 31000:2018. Risk management – Guidelines. Вид. офіц. Geneva : ISO, 2018. 16 с.

48. Xucro G. COBIT 2019-framework-governance-and-management-objectives pages 51-100 - flip PDF download | fliphtml5 | galo xucro. Top FlipBook Maker & Digital Publishing Platform - FlipHTML5. URL: https://fliphtml5.com/qzvfo/unwt/basic/51-100 (дата звернення: 01.12.2025)

49. NIST. Security and privacy controls for information systems and organizations. National Institute of Standards and Technology (NIST), 2020. 465 с. URL: https://doi.org/10.6028/NIST.SP.800-53r5 (дата звернення: 30.11.2025).

50. Temoshok D. Digital identity guidelines. Gaithersburg, MD : National Institute of Standards and Technology, 2025. URL: https://doi.org/10.6028/nist.sp.800-63-4 (дата звернення: 08.12.2025).

51. Center for Internet Security (CIS). CIS benchmarks. 2024. URL: https://www.cisecurity.org/cis-benchmarks (дата звернення: 24.10.2025).

52. Zero trust architecture / S. Rose та ін. National Institute of Standards and Technology, 2020. URL: https://doi.org/10.6028/nist.sp.800-207 (дата звернення: 08.12.2025).

53. ISO/IEC. Information security, cybersecurity and privacy protection – Information security controls. Geneva : ISO/IEC, 2022. 154 с. URL: https://learn.ztu.edu.ua/pluginfile.php/271472/mod_resource/content/2/ISO%202700 2%202022.pdf (дата звернення: 30.11.2025).

54. Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile / N. Alex та ін. National Institute of Standards and Technology (NIST), 2025. 40 с. URL: https://doi.org/10.6028/NIST.SP.800-61r3 (дата звернення: 30.11.2025).

55. Cloud controls matrix and CAIQ v4 | CSA. Home | CSA. URL: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/ (дата звернення: 01.12.2025).

56. OWASP top 10:2021. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/Top10/2021/ (дата звернення: 01.12.2025).

57. ACM code of ethics and professional conduct. ACM. URL: https://www.acm.org/code-of-ethics (дата звернення: 01.12.2025).

58. IBM. IBM security qradar administration guide. 2024. URL: https://www.ibm.com/docs/en/SS42VS_7.5/pdf/b_qradar_admin_guide.pdf (дата звернення: 01.12.2025).

59. Kent K., Souppaya M. Guide to computer security log management. Gaithersburg, MD : National Institute of Standards and Technology, 2006. URL: https://doi.org/10.6028/NIST.SP.800-92 (дата звернення: 01.12.2025).

60. Mitre att&ck®. MITRE ATT&CK®. URL: https://attack.mitre.org/ (дата звернення: 01.12.2025).

61. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 17 лип. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 30.11.2025).

ДОДАТКИ

Додаток А

ПОЛІТИКА ДОПУСТИМОГО ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТОВ “UkrSec”

1. Мета та Призначення

Ця Політика визначає правила безпечного, законного та відповідального використання інформаційних ресурсів Компанії. Мета обробки даних: Забезпечення захисту конфіденційності, цілісності та доступності інформації, виконання контрактних зобов’язань перед клієнтами та захист репутації Компанії.

(Коментар: Реалізація Правової вимоги “Законність мети”. Чітко формулюємо мету зі ст. 6 Закону України “Про захист персональних даних”, що легалізує подальші заходи контролю).

2. Сфера застосування

Політика поширюється на всіх співробітників, підрядників та третіх осіб, які мають доступ до ресурсів Компанії. Вона охоплює використання робочих станцій, електронної пошти, доступу до Інтернету та використання власних пристроїв у робочих цілях.

*(Коментар: Реалізація вимоги **ISO 27001 A.5.10** щодо чіткого визначення меж дії правил).*

3. Етичні гарантії та Приватність

Компанія поважає право співробітників на приватність і дотримується принципів прозорості.

Що моніторимо: Компанія здійснює автоматизований моніторинг трафіку корпоративної електронної пошти та дій на корпоративних серверах виключно з метою виявлення кіберзагроз.

Що НЕ моніторимо: Компанія гарантує технічну неможливість та адміністративну заборону доступу до змісту особливих повідомлень у

месенджерах на власних пристроях співробітників, навіть при їх підключенні до корпоративної мережі.

*(Коментар: Реалізація **Етичної вимоги "Мінімізація втручання"**. Чітке розмежування зон контролю знімає напругу в колективі та вирішує етичний конфлікт, описаний у п. 1.4 та 2.4).*

4. Управління доступом та Парольних захист

Співробітникам заборонено передавати свої облікові дані (логін/пароль) будь-кому.

Вимога: Доступ до корпоративних систем ззовні дозволено виключно з використанням багатофакторної автентифікації.

Технічний контроль: Система налаштована так, що автоматично блокує створення паролів коротших за 12 символів та відхиляє спроби входу без другого фактора.

(Коментар: Реалізація Технічної вимоги "Примусове виконання". Маємо не покладатися на пам'ять людей, а впровадити технічне обмеження (SysSP) через налаштування Identity Provider, як рекомендовано в DBIR 2025 для захисту від крадіжки акаунтів).

5. Використання Штучного Інтелекту

Дозволяється використання інструментів GenAI лише через корпоративні акаунти, надані Компанією.

Суворо заборонено вводити персональні дані клієнтів, фінансову інформацію або фрагменти пропрієтарного вихідного коду в публічній версії чат-ботів.

*(Коментар: Вирішення виявленої проблеми **"Shadow IT"**. Це пряма відповідь на ризику витоку даних через ШІ, про якій йшлося в аналізі DBIR 2025).*

6. Поводження з даними та Пристроями

Заборонено пересилати робочі документи на особисті поштові скриньки.

Технічний контроль: Спроби передачі даних будуть автоматично блокуватися систем DLP.

При використанні власного пристрою співробітник зобов'язаний встановити рекомендований антивірус та пароль блокування екрану.

*(Коментар: Інтеграція **Технічного методу "DLP"** (п. 3.3) у текст політики).*

7. Відповідальність та Інциденти

Співробітник зобов'язаний негайно повідомляти Службу безпеки про підрозділі листи або втрату пристрою.

Санкції: У разі ненавмисної помилки застосовується додаткове навчання. У разі свідомого порушення (наприклад, вимкнення антивірусу) – дисциплінарне стягнення. А у випадках несанкціонованого втручання в роботу систем – до кримінальної відповідальності згідно з Кримінальним кодексом України (ст. 361-363) [61].

*(Коментар: Реалізація **Етичної вимоги "Справедливість".** Диференціація відповідальності сприяє культурі довіри, а не страху)*

8. Згода

Я підтверджую, що ознайомився з цією Політикою, розумію мету моніторингу моєї робочої активності та надаю добровільну згоду на обробку моїх даних в межах, необхідних для забезпечення кібербезпеки.

*(Коментар: Реалізація **Правої вимоги "Згода"**. Отримання підпису перетворює документ на юридично зобов'язуючий, виконуючи вимоги ст. 11 Закону про ПД).*