

Державний торговельно-економічний університет
Кафедра інженерії програмного забезпечення та кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Система захисту конфіденційної інформації на основі багаторівневого аналізу

Студента 1 курсу, 9м групи,
спеціальності 125, «Кібербезпека
та захист інформації», освітньої
програми «Безпека систем
електронних комунікацій в
економіці»

підпис студента

Романько
Вікторії
Володимирівни

Науковий керівник
кандидат економічних
наук, професор кафедри
інженерії програмного
забезпечення та
кібербезпеки

підпис керівника

Чубаєвський
Віталій Іванович

Гарант освітньої програми к.т.н.,
професор кафедри інженерії
програмного забезпечення та
кібербезпеки

підпис керівника

Хохлачова Юлія
Євгенівна

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення та кібербезпеки

Освітній ступінь Магістр

Спеціальність 125 «Кібербезпека за захист інформації»

Освітня програма «Безпека систем електронних комунікацій в економіці

Затверджую

Зав. кафедри інженерії програмного
забезпечення та кібербезпеки

Криворучко О.В.

«13» грудня 2024 р.

Завдання на кваліфікаційну роботу студентіві

Романько Вікторії Володимирівні

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи «Система захисту конфіденційної інформації на основі багаторівневого аналізу»

Затверджена наказом ректора від «27» листопада 2024 р. № 4194

2. Строк здачі студентом закінченого роботи 15 листопада

3. Цільова установка та вихідні дані до роботи

Мета роботи дослідження ефективності застосування системи захисту конфіденційної інформації на основі багаторівневого аналізу.

Об'єкт дослідження є аналіз процесів у системі захисту конфіденційної інформації на основі багаторівневого аналізу

Предмет дослідження – метод використання інструментарію PLEAK на основі PE-
BPMN

4. Консультанти роботи із зазначенням розділів, які консультують:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв

5. Зміст кваліфікаційної роботи (перелік питань за кожним розділом)

ВСТУП

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ

1.1. Поняття та класифікація конфіденційності

1.2. Сучасні методи та засоби захисту інформації

1.3. Огляд нормативних документів та стандартів захисту інформації

1.4. Основи моделювання бізнес-процесів з використанням BPMN (Business Process Model and Notation)

1.5. Висновки до розділу 1

РОЗДІЛ 2. ІНСТРУМЕНТАРІЙ PLEAK ДЛЯ БАГАТОРІВНЕВОГО АНАЛІЗУ

2.1. Архітектура та функціональні можливості PLEAK

2.2. Інтеграція PLEAK з PE-BPMN для багаторівневого аналізу конфіденційності

2.3. Переваги та обмеження застосування PLEAK на основі PE-BPMN

2.4. Висновки до розділу 2

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

3.1. Параметри оцінки ефективності багаторівневого аналізу

3.2. Порівняльний аналіз з іншими методами захисту інформації

3.3. Висновки до розділу 3

РОЗДІЛ 4. АНАЛІЗ ТА РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ СИСТЕМИ

4.1. Ефективність системи захисту конфіденційної інформації

4.2. Недоліки та обмеження системи захисту

4.3. Перспективи розвитку та вдосконалення системи захисту на основі PLEAK та PE-BPMN

4.4. Висновки до розділу 4

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

6. Календарний план виконання роботи

№ пор.	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	
		за планом	фактично
1	2	3	4
1.	<i>Вибір теми кваліфікаційної роботи</i>	<i>07.11.2023</i>	<i>07.11.2023</i>
2.	<i>Розробка та затвердження завдання на кваліфікаційну роботу магістра (стац/заоч)</i>	<i>13.12.2023</i>	<i>13.12.2023</i>
3.	<i>Вступ та перелік літературних джерел</i>	<i>22.02.2024</i>	<i>22.02.2024</i>
4.	<i>Розробка технічного завдання</i>	<i>14.03.2024</i>	<i>14.03.2024</i>
5.	<i>Розділ 1. Теоретичні основи захисту конфіденційності</i>	<i>10.04.2024</i>	<i>10.04.2024</i>
6.	<i>Розділ 2. Інструментарій <i>pleak</i> для багаторівневого аналізу</i>	<i>23.05.2024</i>	<i>23.05.2024</i>
7.	<i>Розділ 3. Дослідження ефективності системи захисту конфіденційної інформації</i>	<i>05.09.2024</i>	<i>05.09.2024</i>
8.	<i>Розділ 4. Аналіз та рекомендації щодо впровадження системи</i>	<i>05.09.2024</i>	<i>05.09.2024</i>
9.	<i>Розробка методики, алгоритму захисту</i>	<i>27.09.2024</i>	<i>27.09.2024</i>
10.	<i>Написання наукової статті</i>	<i>16.04.2024</i>	<i>16.04.2024</i>
11.	<i>Керівництво користувача</i>	<i>11.10.2024</i>	<i>11.10.2024</i>
12.	<i>Висновки та пропозиції</i>	<i>16.10.2024</i>	<i>16.10.2024</i>
13.	<i>Здача кваліфікаційної роботи на кафедрі (перша перевірка)</i>	<i>18.10.2024</i>	<i>18.10.2024</i>
14.	<i>Підготовка автореферату та презентації доповіді</i>	<i>28.10.2024</i>	<i>28.10.2024</i>
15.	<i>Попередній захист кваліфікаційної роботи</i>	<i>29.10.2024– 31.10.2024</i>	<i>29.10.2024– 31.10.2024</i>
16.	<i>Здача зброшурованої кваліфікаційної роботи</i>	<i>15.11.2024</i>	<i>15.11.2024</i>
17.	<i>Зовнішнє рецензування кваліфікаційної роботи</i>	<i>28.10.2024</i>	<i>28.10.2024</i>
18.	<i>Підготовка до публічного захисту кваліфікаційної роботи</i>	<i>02.12.2024- 03.12.2024</i>	<i>02.12.2024- 03.12.2024</i>

7. Дата видачі завдання _____ «13» грудня 2024р.

8. Науковий керівник кваліфікаційної роботи

Чубаєвський Віталій Іванович

(прізвище, ініціали, підпис)

9. Гарант освітньої програми

Хохлачова Ю.Є.

(прізвище, ініціали, підпис)

10. Завдання прийняв до виконання студент _____

Романько В.В.

(прізвище, ініціали, підпис)

12. Висновок про кваліфікаційну роботу

Кваліфікаційна робота студента Романько В.В.

(прізвище, ініціали)

може бути допущена до захисту екзаменаційній комісії.

Гарант освітньої програми Хохлачова Ю.Є.

(прізвище, ініціали, підпис)

Завідувач кафедри Криворучко О.М.

(підпис, прізвище, ініціали)

«13» грудня 2024 р.

ЗМІСТ

ВСТУП.....	11
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ	13
1.1. Поняття та класифікація конфіденційності	13
1.2. Сучасні методи та засоби захисту інформації.....	15
1.3. Огляд нормативних документів та стандартів захисту інформації	21
1.4. Основи моделювання бізнес-процесів з використанням BPMN (Business Process Model and Notation)	24
1.5. Висновки до розділу 1.....	26
РОЗДІЛ 2. ІНСТРУМЕНТАРІЙ PLEAK ДЛЯ БАГАТОРІВНЕВОГО АНАЛІЗУ ..	28
2.1. Архітектура та функціональні можливості PLEAK	28
2.2. Інтеграція PLEAK з PE-BPMN для багаторівневого аналізу конфіденційності	32
2.3. Переваги та обмеження застосування PLEAK на основі PE-BPMN.....	36
2.4. Висновки до розділу 2.....	39
РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ	41
3.1. Параметри оцінки ефективності багаторівневого аналізу	41
3.2. Порівняльний аналіз з іншими методами захисту інформації	43
3.3. Висновки до розділу 3.....	47
РОЗДІЛ 4. АНАЛІЗ ТА РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ СИСТЕМИ	49
4.1. Ефективність системи захисту конфіденційної інформації.....	49
4.2. Недоліки та обмеження системи захисту	53
4.3. Перспективи розвитку та вдосконалення системи захисту на основі PLEAK та PE-BPMN	56

4.4. Висновки до розділу 4.....	60
ВИСНОВКИ ТА ПРОПОЗИЦІЇ	62
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	65

Анотація

У випускній кваліфікаційній роботі здійснено дослідження та аналіз функції системи багаторівневого аналізу конфіденційної інформації. Було розглянуто інструментарій PLEAK на основі PE- BPMN. Результатом роботи є повний аналіз системи захисту конфіденційної інформації на основі багаторівневого аналізу, її функцій, недоліків, переваг та поєднання з іншими допоміжними інструментами.

Ключові слова: аналіз, інструментарій PLEAK, бізнес-процеси, конфіденційність.

Anotation

In the final qualification work, the research and analysis of the function of the system of multilevel analysis of confidential information was carried out. The PLEAK toolkit based on PE-BPMN was considered. The result of the work is a complete analysis of the system of protection of confidential information based on multilevel analysis, its functions, disadvantages, advantages and combination with other auxiliary tools.

Keywords: analysis, PLEAK toolkit, business processes, confidentiality.

ВСТУП

Сучасний період розвитку суспільства характеризується значним зростанням ролі інформації, інформаційних ресурсів, інформаційних технологій, що призводить до активізації інформаційних відносин, які виникають у різних сферах життєдіяльності людини та держави, під час здійснення певного виду діяльності, яка пов'язана з володінням, збиранням, одержанням, зберіганням, користуванням, поширенням відомостей. Конфіденційна інформація, незалежно від того, предметом яких відносин вона виступає, має певну значимість, цінність для суб'єкта інформації. Цінність інформації зумовлена її використанням в публічній сфері – для забезпечення державного управління в різних сферах суспільного життя, в приватній сфері – для реалізації та захисту прав держави, фізичних та юридичних осіб. Отримання такої інформації сторонніми особами може завдати істотної шкоди як інтересам держави, приватним, так і публічним інтересам.

Актуальність обраної теми полягає у збільшенні попиту на захист цінної інформації у зв'язку з посиленням кібератак на підприємства та державні установи. На сьогоднішній день жодна компанія не може існувати без належного захисту конфіденційних даних, особливо в умовах воєнного стану, коли кількість кіберзагроз збільшилась втричі. Зростання обсягів оброблюваної інформації, активне використання мережевих технологій вимагають вдосконалення методів захисту інформації. Одним із ефективних підходів є багаторівневий аналіз захисту, який дозволяє комплексно оцінювати і забезпечувати безпеку даних.

Мета роботи є дослідження ефективності застосування системи захисту конфіденційної інформації на основі багаторівневого аналізу.

Об'єкт дослідження є аналіз процесів у системі захисту конфіденційної інформації на основі багаторівневого аналізу.

Предмет дослідження є метод використання інструментарію PLEAK на основі PE- BPMN.

Наукова новизна. Вперше проведено комплексне дослідження системи захисту конфіденційної інформації з використанням інструментарію PLEAK на основі PE-BPMN. Запропонований підхід дозволяє інтегрувати багаторівневий аналіз конфіденційності в процеси моделювання бізнес-процесів, що забезпечує більш високий рівень захисту інформації.

Методи дослідження. У роботі використовувались наступні методи:

- 1) Аналіз літературних джерел: для вивчення теоретичних основ та сучасних методів захисту інформації;
- 2) Моделювання бізнес-процесів: з використанням BPMN та PE-BPMN для створення моделей бізнес-процесів;
- 3) Експериментальні дослідження: для оцінки ефективності запропонованої системи захисту;
- 4) Порівняльний аналіз: для порівняння запропонованої системи з існуючими методами захисту інформації.

Результати дослідження можуть бути використані для підвищення рівня безпеки конфіденційної інформації в організаціях, а також для подальших наукових досліджень у сфері інформаційної безпеки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ

1.1. Поняття та класифікація конфіденційності

Конфіденційність є складним і багатовимірним поняттям, яке розглядається з різних дисциплінарних перспектив. Загалом, вона охоплює право індивідів або організацій контролювати інформацію про себе і обмежувати доступ до неї. Існують різні типи конфіденційності, які забезпечують різні функції та задовольняють різні психологічні потреби.

За даними дослідження Д. Педерсена, існує шість типів конфіденційності: усамітнення, ізоляція, анонімність, стриманість, близькість з друзями та близькість з родиною. Ці типи забезпечують п'ять основних функцій: автономію, довіру, відновлення, роздуми та творчість [37].

Інформаційна конфіденційність включає контроль над персональною інформацією, зокрема в Інтернеті. Інформаційна конфіденційність залежить від сприйняття контролю над інформацією та ризику її використання. Наприклад, фактори, такі як анонімність і секретність, є засобами контролю інформації [18].

Дослідження показують, що у різних культурах існують різні уявлення про конфіденційність. Наприклад, в Саудівській Аравії більша увага приділяється родинній конфіденційності, тоді як у США наголос робиться на особистій конфіденційності та відносинах з державою [45].

У медичному контексті конфіденційність є важливим питанням. Дослідження показали, що в професійних медичних службах конфіденційність має багатошаровий характер, де існує необхідність збереження секретів як компаній, так і індивідів [25].

З розвитком Інтернету зросла потреба у захисті персональної інформації, що вимагає використання таких методів, як анонімність та псевдонімність для забезпечення безпеки особистих даних [15].

Конфіденційність можна класифікувати за кількома критеріями, залежно від сфери застосування та характеру інформації, що захищається. Основні типи конфіденційності включають:

Таблиця 1.1

ОСНОВНІ ВИДИ КОНФІДЕНЦІЙНОСТІ

Вид конфіденційності	Характеристика
Державна	Захист державних таємниць і інформації, яка є важливою для національної безпеки та функціонування державних органів.
Інформаційна	Охоплює захист даних, що зберігаються в цифровій формі, таких як особисті дані користувачів в інтернеті, дані про поведінку користувачів, повідомлення та інші електронні документи.
Комерційна	Захист комерційної інформації, яка є власністю компанії, включаючи комерційні таємниці, бізнес-плани, фінансові дані та інші чутливі матеріали.
Комунікаційна	Захист інформації, що передається через засоби комунікації, такі як телефонні розмови, електронні листи, текстові повідомлення тощо. Важливою складовою є право на недоторканність листування.
Особиста	Захист особистої інформації, що стосується індивідів, наприклад, ідентифікаційні дані, фінансова інформація, медичні записи тощо. Це також включає право на приватність у повсякденному житті.
Професійна	Включає захист інформації, яка надається професіоналам, таким як лікарі, юристи, бухгалтери, які зобов'язані зберігати конфіденційність інформації своїх клієнтів.
Соціальна	Включає право на приватність у соціальних взаємодіях, таких як право на анонімність в онлайн-платформах та соціальних мережах.
Цифрова	Захист особистих даних в цифровому середовищі, включаючи Інтернет, мобільні додатки та інші електронні платформи. Це також стосується захисту від стеження та несанкціонованого доступу до даних.

Джерело: складено автором на основі [10]

Ця класифікація допомагає краще розуміти різні аспекти конфіденційності та забезпечувати їх відповідний захист залежно від конкретних обставин та контексту.

Конфіденційність є багатограним поняттям, яке охоплює різні аспекти особистого та професійного життя. Її важливість підкреслюється різними дослідженнями, що розглядають питання конфіденційності в контексті інформації, культурних відмінностей та професійної етики.

1.2. Сучасні методи та засоби захисту інформації

Інформація стає одним із найцінніших активів будь-якої організації чи держави, її все більше охороняють і цінують. У той же час ця інформація піддається багатьом загрозам, таким як кібератаки та порушення конфіденційності даних. Тому інформаційна безпека стала одним із найважливіших питань для кожного, хто використовує ІКТ. Варто зазначити, що ці загрози стосуються не лише великих компаній та державних установ, а й звичайних користувачів, які обробляють та зберігають свої дані в Інтернеті.

Інформаційна безпека — це комплексна система заходів, спрямованих на захист інформації від несанкціонованого доступу, розголошення, пошкодження, знищення, зміни або втрати. У сучасну цифрову епоху, коли інформація передається через Інтернет, інформаційна безпека стала ключовим елементом як для організацій, так і для окремих осіб [29].

Автори визначення інформаційної безпеки та кібербезпеки не є однозначними, оскільки обидва терміни сягають корінням у низку наукових галузей, включаючи інформатику, управління та національну безпеку. Одним із перших авторів, які дали визначення терміну кібербезпека, була Дороті Деннінг [17], американський фахівець з комп'ютерної безпеки.

Визначення інформаційної безпеки відноситься до захисту інформації від несанкціонованого доступу, розкриття, пошкодження, знищення, модифікації або

втрати. З іншого боку, кібербезпека більше зосереджена на захисті цифрової інформації та пов'язаних систем від загроз, що виникають з комп'ютерних мереж [21].

З розвитком інформаційних технологій ці терміни почали використовувати як синоніми. Однак між ними є деякі тонкі відмінності. Кібербезпека стосується зусиль із захисту мереж і пов'язаних систем від цифрових загроз, таких як хакери, віруси, DDoS-атаки тощо. Інформаційна безпека, з іншого боку, стосується захисту всіх типів інформації, а не лише тієї, що зберігається в ІТ-системах .

Загроза інформаційній безпеці є серйозною та може призвести до серйозних наслідків, таких як вторгнення в приватне життя, крадіжка особистих даних, втрата комерційної та конфіденційної інформації та навіть репутаційна шкода. Як показують дослідження, витрати, пов'язані з кібератаками, зростають, а їх масштаб і складність продовжують зростати.

Згідно зі звітом IBM Security Cost of a Data Breach Report за 2020 рік, середня вартість витоку даних становила 3,86 мільйона доларів США у 2020 році, що на 1,5 відсотка більше, ніж у попередньому році [28]. Крім того, у Звіті Microsoft про цифровий захист за 2020 рік зазначено, що кіберзлочинність є однією з найбільших загроз для компаній і окремих осіб, і що вартість збитків, пов'язаних з кібератаками, у 2020 році склала понад 1,5 трильйона доларів [36].

У Європі Європейське агентство мережевої та інформаційної безпеки (ENISA) публікує щорічний звіт про мережеві та інформаційні загрози. У своєму звіті про ландшафт загроз за 2021 рік ENISA стверджує, що у 2020 році спостерігалось збільшення кількості зловмисних програм, фішингу та програм-вимагачів, що наголошує на необхідності вжити заходів для покращення інформаційної безпеки.

Інформаційна безпека в даний час є однією з найважливіших проблем для багатьох установ, підприємств і організацій у всьому світі. Атаки на ІТ-системи можуть призвести до втрати конфіденційної інформації, такої як дані клієнтів, співробітників, паролі та інша конфіденційна інформація. За останні роки було

багато випадків атак на інформаційні системи, які викликали хвилю дискусій про необхідність посилення захисту інформації та заходів безпеки.

Одна з найбільших атак на інформаційні системи була на Equifax, яке є одним із трьох найбільших бюро кредитної звітності в Сполучених Штатах. У 2017 році хакери отримали доступ до особистих даних понад 147 мільйонів клієнтів, включаючи номери національного страхування, дати народження, адреси та іншу інформацію. Атака була однією з найбільших в історії та завдала серйозної фінансової та репутаційної шкоди Equifax.

Іншим прикладом стала кібератака на американську компанію Target у 2013 році, яка змусила багато компаній переглянути свій підхід до безпеки. В результаті атаки хакери отримали доступ до даних понад 110 мільйонів клієнтів, включаючи номери кредитних карт і особисту інформацію. Атака завдала збитків на понад 162 мільйони доларів.

Урядові та неурядові організації в усьому світі вживають низку заходів для посилення інформаційної безпеки та захисту від кібератак. У 2018 році Європейське агентство мережевої та інформаційної безпеки (ENISA) опублікувало звіт, у якому визначено кілька ключових ризиків інформаційної безпеки, таких як атаки на критичну інфраструктуру, використання технології блокчейн у злочинних цілях і атаки на хмарні системи. У відповідь на зростаючі загрози країни в усьому світі вживають багатьох заходів для посилення захисту своїх інформаційних систем. У Польщі Агентство внутрішньої безпеки (ABW) співпрацює з різними установами, щоб підвищити обізнаність про кіберзагрози та запобіжні заходи. Агентство проводить тренінги для бізнесу та державних установ, організовує інформаційні кампанії з інформаційної безпеки. У 2020 році РНБО запустило спеціальний сайт «Безпечна компанія», на якому надаються практичні поради та інформація щодо інформаційної безпеки для бізнесу. Інші країни також роблять подібні кроки. У Сполучених Штатах Національний інститут стандартів і технологій (NIST) розробив Рамку кібербезпеки, яка є набором рекомендацій і найкращих практик щодо інформаційної безпеки. У Європі Європейське агентство

мережевої та інформаційної безпеки (ENISA) розробляє рекомендації щодо інформаційної безпеки та організовує навчальні та просвітницькі кампанії. Міжнародні організації також вживають заходів для посилення інформаційної безпеки. Прикладом є НАТО, яка розробила концепцію кіберзахисту та проводить навчання своїх членів з інформаційної безпеки.

Варто зазначити, що захист інформаційних систем і даних є обов'язком не лише держав і організацій, а й окремих користувачів. Приклади хорошої практики включають використання складних паролів, регулярне оновлення програмного забезпечення та обережність під час відкриття підозрілих повідомлень або натискання посилань.

Все більше і більше діяльності переміщується в цифровий світ, ризики інформаційної безпеки становлять серйозний виклик для суспільства в усьому світі. У відповідь на ці виклики країни, організації та окремі користувачі вживають різноманітних заходів для посилення захисту даних та інформаційних систем. Важливо пам'ятати, що дбати про інформаційну безпеку – обов'язок кожного.

Однією з найбільших проблем інформаційної безпеки є відсутність єдиної політики інформаційної безпеки. Кожна країна, організація чи компанія має свій власний підхід до управління інформаційною безпекою. Ці відмінності можуть бути наслідком багатьох факторів, таких як культурні, законодавчі, організаційні чи технологічні відмінності. Недостатньо гармонізований підхід до управління інформаційною безпекою призводить до вразливості інформаційної безпеки, якою може скористатися зловмисник. Тому для країн, організацій або компаній важливо працювати на основі гармонізованих стандартів інформаційної безпеки [35].

Ще одним викликом інформаційній безпеці є загрози, пов'язані з розвитком технологій. З розвитком технологій у зловмисників з'являється все більше можливостей для здійснення кібератак. Прикладом такої загрози є технологія штучного інтелекту, що розвивається, яка дозволяє створювати інструменти для здійснення атак із ще більшою точністю та ефективністю [33]. Крім того, збільшення кількості підключених до мережі пристроїв, таких як пристрої

Інтернету речей, збільшує число потенційних векторів атак. Це вимагає від країн, організацій і компаній постійно працювати над захистом своїх систем від нових типів загроз [14]. Одним із способів вирішення проблем інформаційної безпеки є розробка систем моніторингу та реагування на загрози. Такі системи дають змогу швидко виявляти атаки та вживати відповідних заходів для мінімізації впливу атаки. Крім того, розвиток компетенції та обізнаності співробітників щодо інформаційної безпеки є ключовим для забезпечення ефективного захисту систем. Держави, організації та компанії повинні інвестувати в навчання та освіту з інформаційної безпеки для співробітників, щоб вони могли ефективно захищати свої системи від кіберзагроз [42].

Збільшення кількості кібератак, які стають дедалі прогресивнішими, а також нові загрози, пов'язані з розвитком технологій, вимагають постійного розвитку заходів із забезпечення інформаційної безпеки. Варто розглянути, які перспективи розвитку інформаційної безпеки, які найважливіші напрямки розвитку та яка роль держави та організацій у забезпеченні інформаційної безпеки.

Ключову роль у забезпеченні інформаційної безпеки відіграють держава та організації. У Польщі Агентство внутрішньої безпеки (ABW) відповідає за координацію діяльності, пов'язаної з інформаційною безпекою, а також за здійснення діяльності, пов'язаної із захистом секретної інформації (Swoboda, 2014, с. 303). Крім того, різні державні інституції та відомства відстежують ситуацію з інформаційною безпекою та вживають заходів для запобігання загрозам.

Організаціям також необхідно ефективно захищати свої ІТ-системи від кібератак, які можуть призвести до крадіжки даних, зловмисного програмного забезпечення або пошкодження систем. Для цього їм потрібно використовувати передові технології та практики інформаційної безпеки та проводити регулярні аудити безпеки.

Розвиток інформаційних технологій створює нові можливості, але водночас і нові загрози інформаційній безпеці. З розвитком Інтернету речей (IoT), штучного інтелекту (AI) і блокчейну кількість потенційних атак на інформаційні системи

зростає. Однією з найбільших проблем буде забезпечення безпеки систем, що керують великими обсягами даних, як-от медичні, фінансові дані чи дані, пов'язані з критичною інфраструктурою. Однак розвиток інформаційних технологій також створює нові можливості для забезпечення інформаційної безпеки. Наприклад, штучний інтелект може допомогти виявляти та запобігати атакам, а блокчейн – у захисті систем від несанкціонованого доступу. Крім того, розвиток Інтернету речей (IoT) та інших технологій, пов'язаних з концепцією індустрії 4.0, може дозволити покращити моніторинг та управління IT-системами в режимі реального часу, що, у свою чергу, матиме позитивний вплив на інформаційну безпеку [33].

Навчання та навчання з кібербезпеки також є важливим напрямком розвитку інформаційної безпеки. Знання про загрози та способи їх уникнення мають бути широко поширеними як серед окремих користувачів, так і серед компаній та державних установ. Таким чином, держави та організації повинні інвестувати в навчальні програми та освітні кампанії для підвищення обізнаності про кіберзагрози та способи протидії їм [44].

Держави та організації також відіграють ключову роль у створенні єдиних стандартів інформаційної безпеки, які застосовуватимуться на міжнародному рівні. Багато країн розробляють власні правила інформаційної безпеки, що призводить до неузгодженості та перешкоджає міжнародній співпраці у разі атак на інформаційні системи [32]. Одним із прикладів такої співпраці є Європейська директива мережевих та інформаційних систем (NIS), яка спрямована на забезпечення високого рівня безпеки інформаційних систем у країнах-членах Європейського Союзу [41].

Таким чином, розвиток інформаційних технологій створює як нові загрози, так і можливості для інформаційної безпеки. Держави та організації відіграють ключову роль у забезпеченні безпеки та повинні інвестувати в освіту та навчання, створення єдиних стандартів та впровадження інноваційних технологічних рішень [44].

1.3. Огляд нормативних документів та стандартів захисту інформації

ISO/IEC 27001:2022 — це міжнародний стандарт, який встановлює вимоги до системи управління інформаційною безпекою (СУІБ) [30]. Основною метою цього стандарту є забезпечення впровадження, підтримки та постійного поліпшення системи управління інформаційною безпекою в організації. Він охоплює такі аспекти, як політики безпеки, управління ризиками, заходи контролю та моніторинг інформаційних активів. Стандарт надає організаціям основу для захисту конфіденційної інформації, гарантування цілісності даних і забезпечення доступності інформаційних систем. ISO/IEC 27001 пропонує підхід на основі ризиків для управління інформаційною безпекою. Організації, які впроваджують цей стандарт, проводять ідентифікацію загроз і вразливостей, оцінюють ризики та розробляють заходи контролю для їх зниження. Сертифікація за ISO/IEC 27001 може підвищити довіру клієнтів і партнерів, оскільки демонструє зобов'язання організації щодо захисту інформації.

ISO/IEC 27002:2022 є супутнім стандартом до ISO/IEC 27001 і містить рекомендації щодо заходів контролю безпеки інформації [31]. Цей стандарт надає практичні поради щодо впровадження заходів захисту, які можна адаптувати до конкретних потреб організації. Він охоплює широкий спектр аспектів безпеки, таких як управління активами, управління доступом, криптографія, фізична безпека, захист комунікацій та інші. Кожен розділ ISO/IEC 27002 містить опис конкретного заходу безпеки, його цілі та рекомендації щодо його впровадження. Організації можуть використовувати цей стандарт як довідковий посібник для розробки власних політик і процедур безпеки. Впровадження рекомендацій ISO/IEC 27002 допомагає організаціям зміцнити свою інформаційну безпеку та забезпечити відповідність законодавчим вимогам.

NIST SP 800-53, розроблений Інститутом стандартів і технологій США (NIST), містить каталог заходів контролю безпеки для федеральних інформаційних систем [39]. Цей документ є частиною комплексу документів NIST, що охоплюють

управління ризиками та інформаційну безпеку. SP 800-53 надає набір загальних заходів контролю безпеки, які можуть бути адаптовані до конкретних потреб різних організацій.

Заходи контролю в NIST SP 800-53 поділені на контрольні сім'ї, що охоплюють різні аспекти інформаційної безпеки, включаючи управління доступом, безпеку операцій, планування аварійного відновлення, захист систем і комунікацій, а також моніторинг і аудит. Цей документ є важливим інструментом для організацій, що прагнуть дотримуватися вимог федеральних регуляцій США, таких як FISMA (Federal Information Security Management Act).

GDPR — це регламент Європейського Союзу, який набув чинності 25 травня 2018 року і встановлює вимоги до обробки персональних даних громадян ЄС [23]. Регламент спрямований на захист прав фізичних осіб щодо їхніх персональних даних і надає їм більше контролю над власною інформацією.

GDPR визначає основні принципи обробки даних, включаючи законність, чесність, прозорість, мінімізацію даних, точність, зберігання даних у формі, що дозволяє ідентифікацію суб'єктів даних. Основні вимоги GDPR включають отримання згоди на обробку даних, забезпечення прав суб'єктів даних на доступ до своїх даних, виправлення та видалення інформації, а також право на перенесення даних.

Регламент також передбачає обов'язок повідомляти про порушення захисту даних, дотримання принципу "privacy by design" та "privacy by default". Порушення вимог GDPR можуть призвести до значних штрафів, що стимулює організації серйозно ставитися до захисту персональних даних.

Директива NIS є першим законодавчим актом Європейського Союзу, спрямованим на забезпечення високого рівня безпеки мереж та інформаційних систем у всьому ЄС [19]. Прийнята в липні 2016 року, директива вимагає від країн-членів ЄС впровадження національних стратегій з кібербезпеки, а також створення механізмів для співпраці між державами. Директива NIS зобов'язує операторів основних послуг (ОПП) і постачальників цифрових послуг (ПДП) дотримуватися

вимог щодо безпеки та повідомлення про інциденти. Основні послуги включають енергетику, транспорт, банківську справу, охорону здоров'я, постачання води та інші критично важливі сектори. Постачальники цифрових послуг включають онлайн-ринків, онлайн-пошукові системи та послуги хмарних обчислень. Цей законодавчий акт має на меті підвищити загальну стійкість ЄС до кіберзагроз.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" регулює відносини у сфері захисту інформації, яка обробляється в інформаційно-телекомунікаційних системах [7]. Він визначає основні принципи захисту інформації, включаючи забезпечення конфіденційності, цілісності та доступності інформації. Закон встановлює вимоги до суб'єктів, які здійснюють обробку інформації, зокрема щодо технічного та організаційного захисту. Закон також передбачає категоризацію інформації за рівнем конфіденційності та відповідні заходи захисту для кожної категорії. Зокрема, визначено процедури акредитації та сертифікації систем захисту інформації, а також відповідальність за порушення вимог закону. Закон є ключовим елементом правової бази захисту інформації в Україні.

Закон України "Про захист персональних даних" регулює обробку персональних даних в Україні, визначаючи права суб'єктів даних та обов'язки володільців і розпорядників баз даних [8]. Основною метою закону є забезпечення захисту прав і свобод людини при обробці персональних даних, зокрема права на приватність. Закон передбачає обов'язок отримання згоди на обробку персональних даних, обмеження щодо обробки спеціальних категорій даних, таких як дані про здоров'я, політичні погляди та інші. Він також визначає права суб'єктів даних на доступ до своїх даних, їх виправлення, видалення та заперечення проти обробки. Важливим аспектом є вимога забезпечення належного захисту персональних даних від несанкціонованого доступу та інших загроз.

ДСТУ 3396.0-96 є національним стандартом України, який встановлює основні положення технічного захисту інформації. Стандарт охоплює комплекс заходів та засобів, спрямованих на захист інформації від несанкціонованого

доступу, витоку, модифікації або знищення [3]. Цей стандарт визначає вимоги до організації системи технічного захисту інформації, включаючи правила класифікації інформаційних ресурсів, ідентифікацію загроз та оцінку ризиків. Він також надає рекомендації щодо вибору та впровадження технічних засобів захисту, таких як шифрування, антивірусні програми, системи виявлення вторгнень та інші. Стандарт є основою для створення системи технічного захисту інформації в організаціях різних секторів.

Ці документи і стандарти надають рамки для створення та підтримки систем захисту інформації в організаціях різних секторів. Вони встановлюють обов'язкові вимоги, найкращі практики та рекомендації, що допомагають забезпечити конфіденційність, цілісність та доступність інформації.

1.4. Основи моделювання бізнес-процесів з використанням BPMN (Business Process Model and Notation)

BPMN (Business Process Model and Notation) — це графічний стандарт для опису та моделювання бізнес-процесів [13]. Він призначений для того, щоб забезпечити загальноприйнятту нотацію, зрозумілу як для технічних користувачів (наприклад, аналітиків та розробників), так і для нетехнічних користувачів (бізнес-користувачів).

Основні елементи BPMN наведені на рис. 1.1.

BPMN дозволяє моделювати складні процеси в організаціях, забезпечуючи ясність та прозорість. Ця нотація використовується для аналізу, документування та вдосконалення процесів, а також для створення специфікацій для автоматизації бізнес-процесів. Завдяки своїй стандартності та зрозумілості, BPMN допомагає уникнути неоднозначностей у спілкуванні між різними учасниками проекту.

Події	Початкова подія
	Проміжна подія
	Кінцева подія
Діяльності	Завдання
	Підпроцес
Потоки	Послідовний потік
	Умова потоку
Гейтвеї	Ексклюзивний гейтвей
	Паралельний гейтвей
Артефакти	Дата
	Групи
Ролі	Пули
	Доріжки

Рис. 1.1. Основні елементи BPMN

Джерело: складено автором на основі [13]

Основна мета BPMN — надати простий і зручний спосіб опису бізнес-процесів, що забезпечує їх зрозумілість на всіх рівнях організації. BPMN дозволяє моделювати процеси з різною деталізацією: від високорівневого огляду до детального опису кожного кроку. Завдяки цьому стандарту користувачі можуть легко створювати діаграми, які ілюструють послідовність завдань, правила прийняття рішень, взаємодії між учасниками процесу та інші аспекти бізнес-процесів.

Однією з ключових особливостей BPMN є його здатність моделювати як прості, так і складні процеси. BPMN надає широкий набір елементів, які дозволяють описувати різні аспекти процесу. Наприклад, "події" у BPMN можуть позначати початок, закінчення або певний момент у процесі, тоді як "діяльності" представляють окремі завдання або операції. Гейтвеї використовуються для

представлення точок прийняття рішень, де процес може розгалужуватися або об'єднуватися. Ці елементи дозволяють моделювати як лінійні, так і розгалужені процеси з численними альтернативами.

BPMN також забезпечує механізм для відображення взаємодії між різними організаційними одиницями чи ролями через використання так званих "пулів" і "доріжок". Пули представляють окремі організації або підрозділи, а доріжки — окремі ролі або групи в межах цих організацій. Такий підхід дозволяє чітко відобразити відповідальність кожного учасника процесу та їх взаємодію з іншими.

Ще однією важливою функцією BPMN є можливість відображення умовних шляхів і паралельного виконання завдань. Це досягається за допомогою використання умовних і паралельних гейтвеїв. Умовні гейтвеї дозволяють моделювати процеси, які можуть мати різні результати на основі певних умов, тоді як паралельні гейтвеї дозволяють показати одночасне виконання кількох завдань. Це особливо корисно для моделювання складних бізнес-процесів, які включають множинні альтернативи та паралельні дії.

Таким чином, BPMN є потужним інструментом для моделювання бізнес-процесів, який забезпечує гнучкість і точність у відображенні реальних процесів. Це робить його незамінним для аналізу, оптимізації та автоматизації процесів, допомагаючи організаціям досягати більшої ефективності та прозорості в їх операційній діяльності.

1.5. Висновки до розділу 1

Конфіденційність є багатовимірним поняттям, що охоплює право на контроль над інформацією. Її класифікація включає державну, інформаційну, комерційну, комунікаційну, особисту, професійну, соціальну та цифрову сфери. Такий підхід дозволяє враховувати специфіку кожного виду конфіденційності для забезпечення їх ефективного захисту в різних контекстах.

Сучасна інформаційна безпека спирається на використання багаторівневих підходів, зокрема криптографії, анонімізації даних і систем управління доступом. Відсутність єдиної політики інформаційної безпеки залишається викликом, однак стандарти, як-от ISO/IEC 27001, сприяють уніфікації підходів.

Нормативна база охоплює міжнародні та національні стандарти, включаючи ISO/IEC 27001, NIST SP 800-53, GDPR, які формують рамки для організації ефективного захисту даних. Важливим залишається дотримання стандартів задля зниження ризиків витоків інформації та порушення конфіденційності.

BPMN є ефективним інструментом для моделювання бізнес-процесів завдяки його універсальності та здатності описувати як прості, так і складні процеси. Його використання дозволяє забезпечити прозорість, що є ключовим для впровадження заходів захисту конфіденційності.

РОЗДІЛ 2. ІНСТРУМЕНТАРІЙ PLEAK ДЛЯ БАГАТОРІВНЕВОГО АНАЛІЗУ

2.1. Архітектура та функціональні можливості PLEAK

PLEAK (Privacy Language Enforcement for Access Control and Key Management) — це комплексна структура, розроблена для забезпечення конфіденційності в обробці даних шляхом застосування політики конфіденційності та безпечного керування криптографічними ключами. Архітектура PLEAK побудована навколо кількох ключових компонентів, кожен з яких відіграє важливу роль у підтримці конфіденційності та безпеки. В основі PLEAK лежить рівень політики конфіденційності, де визначаються детальні політики конфіденційності. Ці політики визначають умови, за яких дані можуть бути доступні та оброблені, використовуючи офіційну мову конфіденційності, яка забезпечує точність і ясність. Цей рівень має вирішальне значення для узгодження практики обробки даних із правовими та організаційними вимогами щодо конфіденційності.

Таблиця 2.1

АРХІТЕКТУРА PLEAK

Складова архітектури	Характеристика
Рівень політики конфіденційності	Відповідає за визначення політики конфіденційності, яка визначає умови, за яких дані можуть бути доступні та оброблені. Ці політики виражені з використанням офіційної мови конфіденційності, яка допускає однозначні визначення. Рівень політики конфіденційності гарантує, що обробка відповідає вимогам конфіденційності.
Управління ключами	Важливим аспектом PLEAK є безпечне керування криптографічними ключами, які використовуються для шифрування даних. Компонент керування ключами забезпечує створення, зберігання, розповсюдження та відкликання ключів. Це гарантує, що ключі доступні лише авторизованим особам і що ними керують у безпечний та сумісний спосіб.

Складова архітектури	Характеристика
Механізми примусу	<p>PLEAK містить механізми примусу, які забезпечують дотримання визначеної політики конфіденційності. Ці механізми включають:</p> <ol style="list-style-type: none"> 1. Контроль доступу – цей компонент контролює, хто може отримати доступ до даних і за яких умов. Він забезпечує виконання правил на основі ролей, атрибутів користувача та контекстної інформації. 2. Анонімізація та маскуванню даних – для захисту конфіденційної інформації використовуються такі методи, як анонімізація та маскуванню даних. Ці методи гарантують, що навіть якщо доступ до даних здійснюється без авторизації, їх неможливо відстежити до окремих суб'єктів. 3. Ведення журналів і аудит – PLEAK веде журнали доступу до даних і обробки даних. Ці журнали використовуються з метою перевірки дотримання політики конфіденційності.
Контроль потоку даних	<p>PLEAK містить механізми для контролю потоку даних у системі та між системами. Це включає визначення того, як дані можуть передаватись, надавати спільний доступ або оброблятися різними компонентами та системами. Контроль потоку даних важливий для запобігання несанкціонованому розповсюдженню даних і забезпечення обробки даних відповідно до політики конфіденційності.</p>
Інтерфейс користувача та адміністрування	<p>Платформа PLEAK надає адміністраторам і користувачам інтерфейс користувача для керування параметрами конфіденційності, визначення політик і моніторингу обробки даних. Цей інтерфейс розроблений таким чином, щоб бути зручним для користувача, що дозволяє користувачам легко налаштовувати та керувати налаштуваннями конфіденційності.</p>

Джерело: складено автором на основі [20; 43]

Механізми забезпечення виконання в PLEAK гарантують суворе дотримання визначеної політики конфіденційності. Ці механізми включають контроль доступу, який керує тим, хто може отримати доступ до даних на основі ролей, атрибутів

користувачів і контекстних факторів. Крім того, PLEAK використовує методи анонізації та маскування даних для захисту конфіденційної інформації, гарантуючи, що несанкціонований доступ до даних не порушить конфіденційність особи. Платформа також включає можливості журналювання та аудиту, які записують доступ до даних і дії з обробки. Ці журнали є безцінними для цілей аудиту, дозволяючи організаціям перевірити дотримання політики конфіденційності.

Важливим аспектом PLEAK є надійний компонент керування ключами, який контролює генерацію, зберігання, розповсюдження та відкликання криптографічних ключів. Це гарантує, що ключі шифрування обробляються безпечно та доступні лише авторизованим особам, таким чином зберігаючи конфіденційність даних.

PLEAK також містить механізми контролю потоку даних, які керують переміщенням даних у системі та між системами, запобігаючи несанкціонованому розповсюдженню та забезпечуючи дотримання політики конфіденційності.

Інтерфейс користувача та інструменти адміністрування, надані PLEAK, пропонують інтуїтивно зрозумілу платформу для керування налаштуваннями конфіденційності, визначення політик і моніторингу активності даних. Цей інтерфейс розроблено таким чином, щоб бути зручним для користувача, що дозволяє адміністраторам і користувачам легко орієнтуватися в складнощах керування конфіденційністю.

Функціональні можливості PLEAK поширюються на забезпечення дотримання політики конфіденційності в режимі реального часу, забезпечуючи безперервну та динамічну відповідність доступу та обробки даних встановленим правилам, навіть якщо політики та контексти змінюються.

Функціональні можливості PLEAK відображені на рис. 2.1.

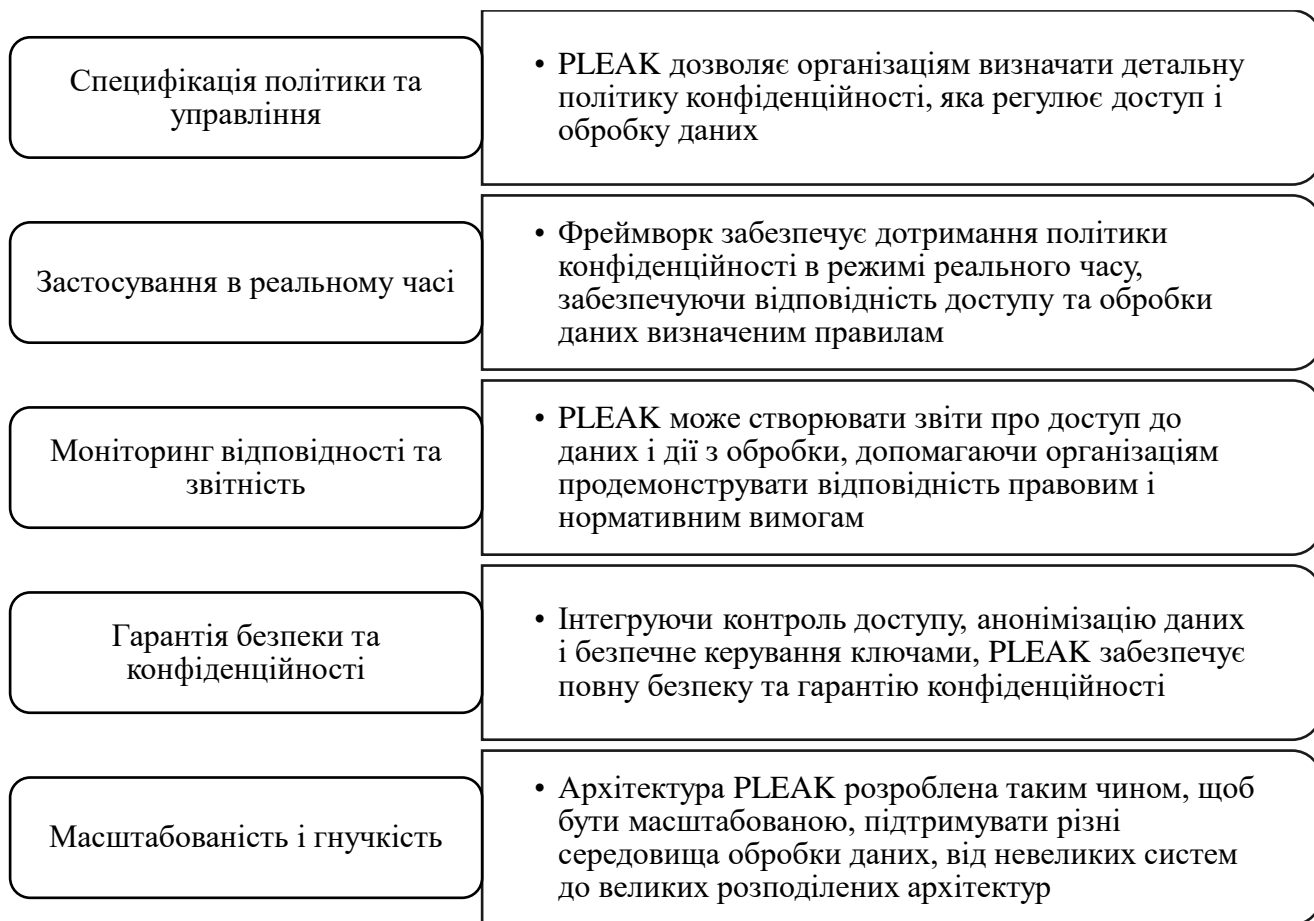


Рис. 2.1. Функціональні можливості PLEAK

Джерело: складено автором на основі [26]

PLEAK не тільки полегшує специфікацію та керування політиками конфіденційності, але також підтримує виконання в режимі реального часу, моніторинг відповідності та звітність. Інтеграція системи контролю доступу, анонімізації даних і безпечного керування ключами забезпечує комплексне рішення для забезпечення конфіденційності та безпеки. Розроблений як масштабований і гнучкий, PLEAK може адаптуватися до різних середовищ обробки даних, що робить його придатним як для малих систем, так і для великих розподілених архітектур. Його гнучкість дозволяє організаціям налаштовувати політику конфіденційності та механізми забезпечення відповідно до своїх конкретних потреб, що робить PLEAK універсальним і потужним інструментом у сфері управління конфіденційністю даних.

2.2. Інтеграція PLEAK з PE-BPMN для багаторівневого аналізу конфіденційності

Інтеграція PLEAK (застосування мови конфіденційності для контролю доступу та керування ключами) з PE-BPMN (модель і нотація бізнес-процесу з покращеною конфіденційністю) пропонує комплексний підхід до багаторівневого аналізу конфіденційності в бізнес-процесах. Ця інтеграція дозволяє організаціям не лише моделювати бізнес-процеси з акцентом на конфіденційність, але й запроваджувати політику конфіденційності та безпечно керувати даними на різних рівнях організації. PE-BPMN розширює стандарт BPMN шляхом включення елементів, пов'язаних із конфіденційністю, у моделі процесів, дозволяючи чітко представити вимоги та проблеми щодо конфіденційності. Завдяки інтеграції PLEAK з PE-BPMN політику конфіденційності, визначену в PLEAK, можна безпосередньо пов'язати з конкретними елементами моделей бізнес-процесів. Наприклад, PE-BPMN можна використовувати для анотування процесів метаданими, пов'язаними з конфіденційністю, такими як рівні конфіденційності даних, згода суб'єкта даних і юридичні зобов'язання. Ці анотації забезпечують чіткий і структурований спосіб фіксації та передачі вимог щодо конфіденційності протягом усього життєвого циклу бізнес-процесів.

Інтеграція полегшує багаторівневий аналіз конфіденційності шляхом узгодження дизайну процесу з механізмами забезпечення конфіденційності. На високому рівні PE-BPMN дозволяє візуалізувати аспекти конфіденційності в бізнес-процесах, дозволяючи зацікавленим сторонам визначити потенційні ризики конфіденційності та області, які потребують особливої уваги. Наприклад, модель може підкреслити, де обробляються або передаються конфіденційні дані, допомагаючи оцінити відповідність нормативним вимогам, таким як GDPR.

Щоб інтегрувати PLEAK з PE-BPMN для багаторівневого аналізу конфіденційності, ми можемо концептуалізувати інтеграцію як багатопланову модель, яка узгоджує моделювання бізнес-процесів із механізмами забезпечення

конфіденційності. Це включає в себе кілька ключових компонентів: моделювання бізнес-процесів (з використанням PE-BPMN), визначення та застосування політики конфіденційності (з використанням PLEAK) і моніторинг відповідності конфіденційності. Нижче наведено детальне пояснення з ілюстративною схемою та таблицею, що підсумовує точки інтеграції.

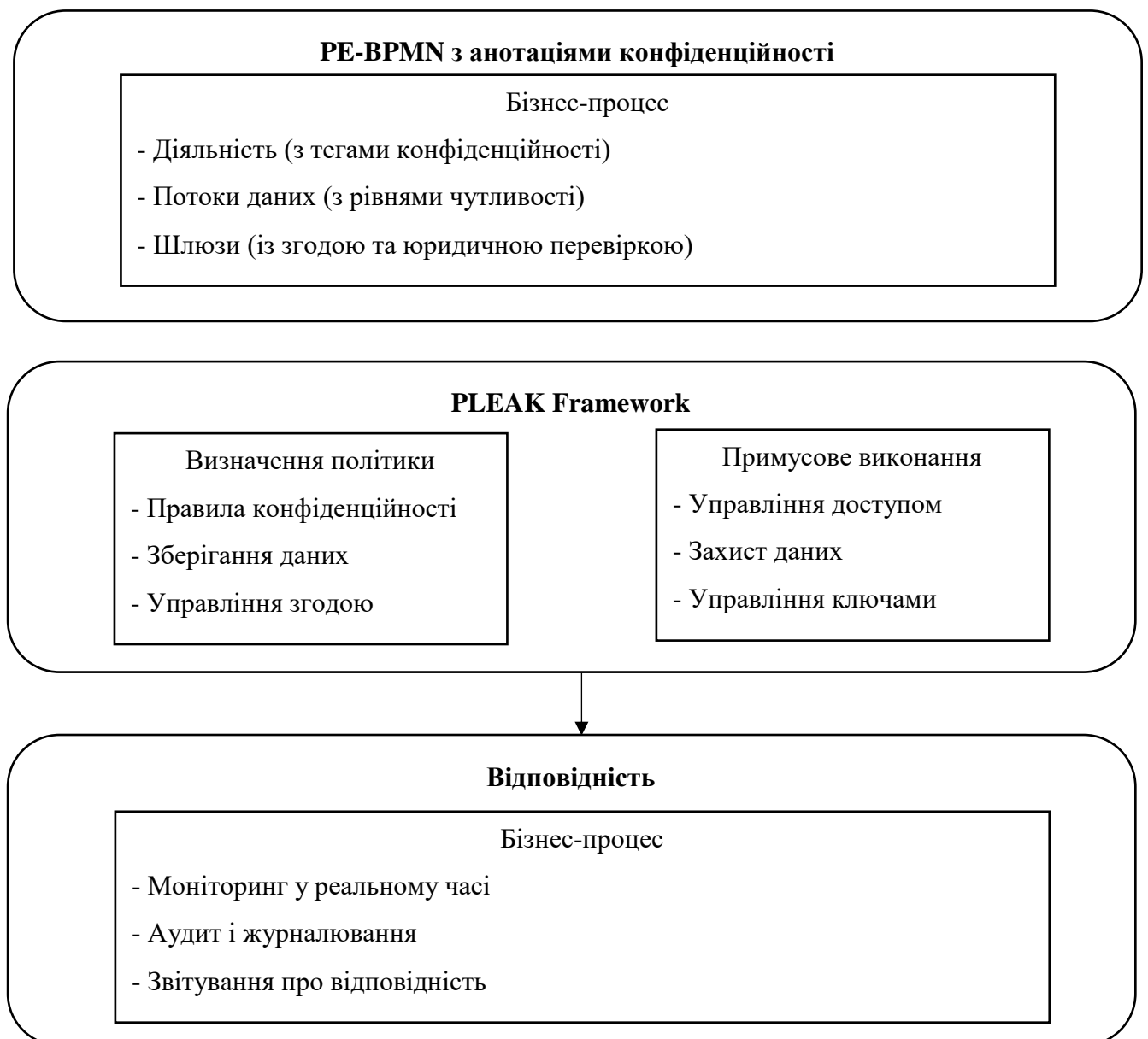


Рис. 2.2. Інтеграційна структура PLEAK з PE-BPMN для багаторівневого аналізу конфіденційності

Джерело: складено автором

На більш детальному рівні механізми примусового виконання PLEAK можна відобразити на цих моделях, щоб гарантувати, що політики контролю доступу, заходи анонімізації даних і методи безпечного керування ключами реалізуються належним чином на кожному етапі процесу.

Крім того, комбіноване використання PE-BPMN і PLEAK дозволяє здійснювати моніторинг у режимі реального часу та перевірку дотримання конфіденційності.

Під час виконання бізнес-процесів PLEAK може застосовувати політику конфіденційності, пов'язану з конкретними процесами, забезпечуючи обробку даних відповідно до попередньо визначених правил. Цей контроль у режимі реального часу допомагає запобігти несанкціонованому доступу та зловживанню даними, тим самим захищаючи конфіденційну інформацію.

Крім того, інтеграція підтримує комплексне ведення журналів і аудит, забезпечуючи детальний запис доступу до даних і дій з обробки. Ці журнали можна використовувати для аналізу після обробки, допомагаючи організаціям перевіряти відповідність і розслідувати потенційні порушення конфіденційності.

Таблиця 2.2

ТАБЛИЦЯ ТОЧОК ІНТЕГРАЦІЇ

PE-BPMN елемент	PLEAK інтеграція	Функціональність
Рівні чутливості даних	Визначення політики (політика чутливості)	Визначення правил на основі конфіденційності даних
Індикатори згоди	Управління згодою	Перевірка реєстрації та дотримання згоди
Правові вимоги	Перевірка відповідності законодавству	Забезпечення обробки відповідно до вимог законодавства
Теги конфіденційності	Заходи захисту даних (анонімізація, маскування)	Впровадження необхідних заходів захисту даних
Діяльність із загрозою конфіденційності	Правила контролю доступу	Контроль доступу на основі ролей користувачів і конфіденційності даних

PE-BPMN елемент	PLEAK інтеграція	Функціональність
Потоки даних	Управління ключами	Захист даних за допомогою шифрування та керування ключами
Шлюзи (точки прийняття рішення)	Застосування політики в реальному часі	Динамічне застосування політик на основі контексту

Джерело: складено автором на основі [26; 43]

PE-BPMN дозволяє детально моделювати бізнес-процеси з великим акцентом на аспектах конфіденційності. Наприклад, коли бізнес-процес передбачає збір даних клієнтів, PE-BPMN може вказати рівень конфіденційності цих даних і будь-яку необхідну згоду. Ця анотація допомагає зрозуміти, де обробляються конфіденційні дані та які заходи конфіденційності необхідно вжити. PLEAK інтегрується з PE-BPMN, застосовуючи політики, визначені в анотаціях конфіденційності. Наприклад, якщо PE-BPMN вказує, що зібрані дані потрібно анонімізувати, PLEAK гарантує застосування відповідних методів анонімізації даних. Крім того, правила контролю доступу, визначені в PLEAK, можна пов'язати з діяльністю в PE-BPMN, забезпечуючи доступ до конфіденційних даних лише авторизованому персоналу. Інтеграція також включає рівень моніторингу, де дотримання політики конфіденційності відстежується в режимі реального часу. Функції журналювання та аудиту PLEAK записують усі дії щодо доступу до даних і обробки, які потім перевіряються на відповідність політикам конфіденційності та нормам. Це особливо важливо для організацій, яким потрібно продемонструвати дотримання законів про захист даних, таких як GDPR.

Цей інтегрований підхід не тільки гарантує, що питання конфіденційності враховуються в розробці бізнес-процесів, але й що ці міркування ефективно дотримуються та контролюються під час виконання процесів. Цей багаторівневий механізм аналізу та забезпечення дотримання правил допомагає організаціям

комплексно керувати ризиками конфіденційності та зміцнювати довіру своїх клієнтів, забезпечуючи конфіденційність і захист даних.

Загалом, інтеграція PLEAK з PE-BPMN створює надійну структуру для управління бізнес-процесами з урахуванням конфіденційності. Це дозволяє організаціям моделювати, запроваджувати та контролювати вимоги щодо конфіденційності на багатьох рівнях, гарантуючи, що міркування щодо конфіденційності впроваджуються в розробку та виконання бізнес-процесів. Цей цілісний підхід не тільки підвищує безпеку та конфіденційність даних, але й допомагає організаціям зміцнювати довіру між зацікавленими сторонами, демонструючи прихильність захисту особистої інформації.

2.3. Переваги та обмеження застосування PLEAK на основі PE-BPMN

Інтеграція PLEAK з PE-BPMN дозволяє повністю вбудовувати питання конфіденційності безпосередньо в моделі бізнес-процесів. Це гарантує, що політика конфіденційності не тільки визначена, але й візуально представлена та дотримується протягом життєвого циклу процесу, сприяючи узгодженому підходу до управління конфіденційністю.

Чітко ануючи бізнес-процеси інформацією, пов'язаною з конфіденційністю, як-от конфіденційність даних і вимоги щодо згоди, PE-BPMN полегшує розуміння та передачу наслідків конфіденційності. Ця прозорість допомагає зацікавленим сторонам, зокрема спеціалістам із відповідності та органам із захисту даних, оцінювати, чи відповідають процеси юридичним і організаційним стандартам конфіденційності.

Здатність PLEAK застосовувати політику конфіденційності в режимі реального часу гарантує, що доступ і обробка даних завжди дотримуються визначених правил. Однак при цьому, застосування політики конфіденційності в реальному часі може призвести до накладних витрат з точки зору часу обробки та продуктивності системи. Для процесів, які включають великі обсяги даних або

вимагають високошвидкісних операцій, ці накладні витрати можуть вплинути на ефективність і пропускну здатність.

Цей динамічний контроль має вирішальне значення для збереження конфіденційності, особливо в середовищах, де дані постійно змінюються та до них мають доступ кілька сторін.

Дизайн фреймворку дозволяє масштабувати його відповідно до потреб організації. Незалежно від того, чи йдеться про невеликі процеси чи складні розподілені системи, PLEAK може адаптуватися до різних рівнів складності та чутливості даних. Крім того, його гнучкість дозволяє налаштовувати політику конфіденційності та механізми забезпечення відповідно до конкретних вимог бізнесу. Функції журналювання та аудиту PLEAK забезпечують детальний запис дій з обробки даних, що є неоціненним для демонстрації відповідності положенням про конфіденційність, таким як GDPR. Ця можливість не тільки підтримує внутрішні аудити, але й допомагає реагувати на нормативні запити та порушення даних.

Забезпечуючи структурований спосіб виявлення ризиків конфіденційності та керування ними, інтеграція PLEAK із PE-BPMN допомагає організаціям завчасно вирішувати потенційні проблеми конфіденційності. Це зменшення ризику є життєво важливим для захисту репутації організації та уникнення юридичних санкцій.

Крім того, інтеграція PLEAK із PE-BPMN може бути складною, вимагаючи глибокого розуміння як правил конфіденційності, так і технічних аспектів моделювання процесів і забезпечення виконання. Ця складність може вимагати спеціальних знань і навичок, що може стати проблемою для організацій, яким бракує цих ресурсів. Комплексний характер структури означає, що значні ресурси можуть знадобитися для впровадження, обслуговування та постійного моніторингу. Це включає фінансові інвестиції в технології, а також час і зусилля персоналу, який бере участь у розробці та забезпеченні політики конфіденційності.

Незважаючи на те, що PLEAK є гнучким, бізнес-середовище, яке швидко змінюється, або нормативно-правове середовище, яке не є досконалим, все ще можуть створювати проблеми. Організаціям необхідно постійно оновлювати політику конфіденційності та механізми забезпечення, щоб йти в ногу з новими вимогами, які можуть бути вимогливими та ресурсомісткими.

Ефективність системи значною мірою залежить від точності та повноти моделей бізнес-процесів і анотацій конфіденційності в PE-BPMN. Неточні або неповні моделі можуть призвести до недостатнього захисту конфіденційності, оскільки певні аспекти обробки даних можуть бути недостатньо охоплені. Хоча PLEAK розроблено для масштабування, надзвичайно великомасштабні реалізації можуть зіткнутися з проблемами, пов'язаними з системною інтеграцією, синхронізацією даних і підтримкою узгодженого виконання в різноманітних і розподілених системах.

В цілому на основі проведеного дослідження, можемо відобразити переваги та обмеження застосування PLEAK на основі PE-BPMN у вигляді рис. 2.3.



Рис. 2.3. Переваги та обмеження застосування PLEAK на основі PE-BPMN

Джерело: складено автором

Підводячи підсумок, хоча інтеграція PLEAK з PE-BPMN пропонує надійний захист конфіденційності та переваги відповідності, вона також створює проблеми, пов'язані зі складністю, вимогами до ресурсів і потенційними накладними витратами на систему. Організації повинні зважити ці переваги та обмеження, розглядаючи можливість прийняття цієї основи.

2.4. Висновки до розділу 2

PLEAK (Privacy Language Enforcement for Access Control and Key Management) пропонує комплексний підхід до забезпечення конфіденційності даних, що охоплює кілька ключових аспектів: управління ключами, контроль доступу, анонімізацію даних та ведення аудиту. Основним компонентом архітектури є рівень політик конфіденційності, який забезпечує створення та управління чіткими правилами захисту даних. Ці політики виражаються мовою конфіденційності, яка дозволяє однозначно визначити умови доступу до даних. Ключовою особливістю PLEAK є його здатність забезпечувати відповідність політик у режимі реального часу, зберігаючи високий рівень гнучкості для інтеграції з існуючими бізнес-процесами.

Функціональні можливості PLEAK також включають механізми примусового виконання політик, які забезпечують суворе дотримання встановлених правил. Це включає шифрування даних, управління криптографічними ключами та контроль потоків даних. Важливим компонентом є журналювання та аудит доступу, що дозволяє організаціям забезпечувати відповідність нормативним вимогам. Усе це сприяє створенню надійної системи, яка не лише захищає конфіденційну інформацію, але й забезпечує прозорість дій з обробки даних, підвищуючи довіру користувачів і партнерів.

Інтеграція PLEAK із PE-BPMN (Privacy-Enhanced Business Process Model and Notation) дозволяє узгодити моделювання бізнес-процесів із реальними механізмами забезпечення конфіденційності. PE-BPMN розширює стандарт BPMN

шляхом додавання елементів, які враховують аспекти конфіденційності, такі як рівні чутливості даних, умови згоди та відповідність правовим вимогам. Інтеграція з PLEAK дозволяє автоматично застосовувати політики конфіденційності до кожного елемента бізнес-процесу, забезпечуючи високий рівень захисту на всіх етапах обробки даних.

Цей підхід сприяє багаторівневому аналізу конфіденційності, забезпечуючи ідентифікацію та усунення ризиків ще на етапі проектування процесу. Наприклад, інтеграція дозволяє відслідковувати, де і як обробляються конфіденційні дані, забезпечуючи їх відповідність регуляторним вимогам, таким як GDPR. Крім того, система в режимі реального часу контролює, щоб дії з обробки відповідали визначеним політикам конфіденційності, що значно зменшує ризики порушення даних.

Основною перевагою застосування PLEAK на основі PE-BPMN є можливість інтеграції бізнес-процесів із заходами захисту конфіденційності. Це дозволяє забезпечити узгодженість між нормативними вимогами та реальними операціями, підвищуючи ефективність управління конфіденційною інформацією. Додатково, автоматизація політик захисту мінімізує людський фактор і дозволяє швидко адаптувати процеси до змін у законодавстві або бізнес-середовищі. Інтеграція з PE-BPMN робить систему доступною для моделювання навіть складних процесів з багатьма точками контролю.

Однак є і певні обмеження. Високі вимоги до технічних ресурсів, необхідних для реалізації та підтримки системи, можуть обмежити її використання у малих і середніх підприємствах. Крім того, успішна інтеграція потребує значних інвестицій у навчання персоналу та адаптацію інструментів до специфіки бізнес-процесів. Ці фактори можуть стати перешкодою для широкого впровадження системи без додаткової оптимізації та зниження витрат на реалізацію.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

3.1. Параметри оцінки ефективності багаторівневого аналізу

Оцінюючи ефективність багаторівневого аналізу конфіденційності, вкрай важливо враховувати різні параметри, які вимірюють, наскільки добре реалізуються та забезпечуються політика конфіденційності та захист. Ці параметри допомагають визначити надійність заходів конфіденційності та визначити області, які потрібно покращити. Ключові параметри оцінки відображені на рис. 3.1.

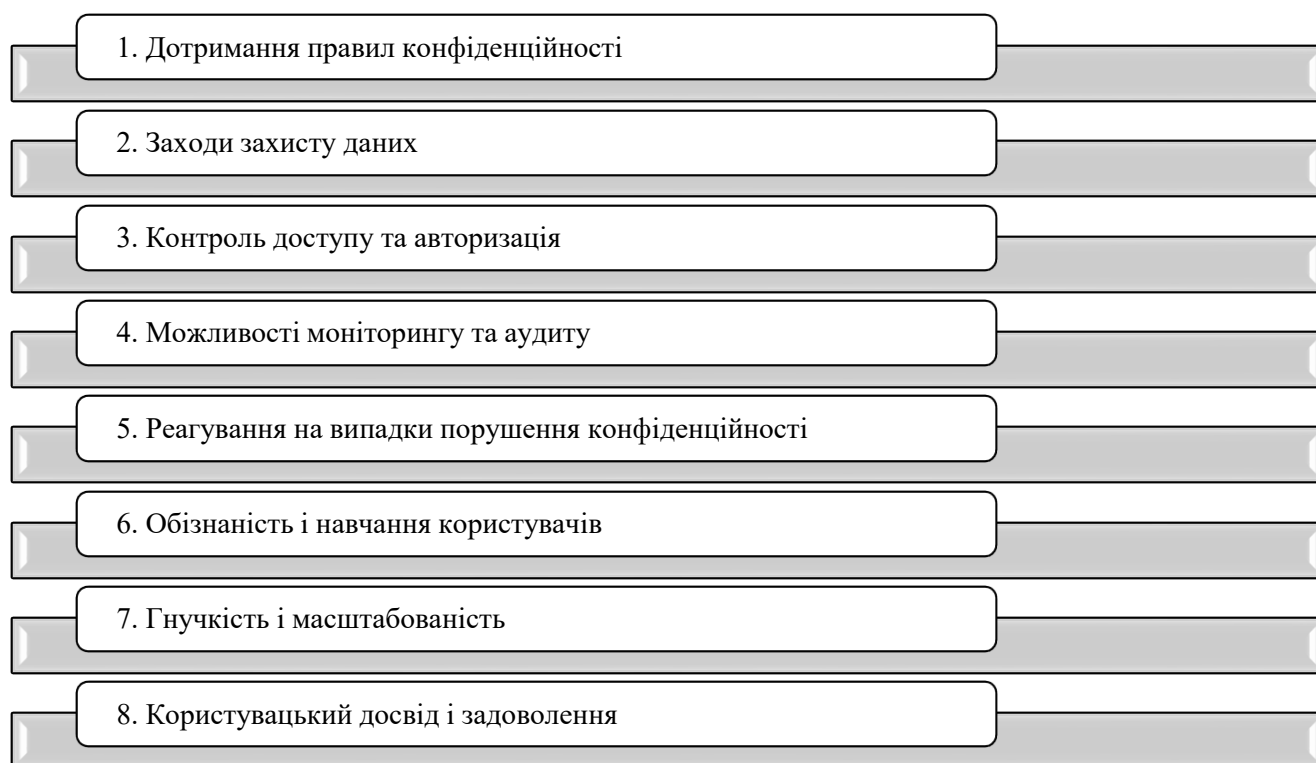


Рис. 3.1. Ключові параметри оцінки ефективності багаторівневого аналізу

Джерело: складено автором на основі [24; 34]

Одним із найважливіших параметрів є забезпечення відповідності системи відповідним законам і нормам щодо конфіденційності, таким як GDPR, HIPAA або

ССРА. Це включає перевірку відповідності діяльності з обробки даних вимогам законодавства щодо згоди, збереження даних і прав суб'єктів даних.

Відповідність стандартам зазвичай вимірюється за допомогою перевірок і переглядів політики та практики конфіденційності.

Заходи захисту даних оцінюють впровадження та ефективність методів захисту даних, таких як шифрування, анонімізація та маскування даних. Мета полягає в тому, щоб забезпечити належний захист конфіденційних даних від несанкціонованого доступу та розголошення.

Оцінка контролю доступу передбачає вивчення механізмів, які використовуються для регулювання того, хто має доступ до даних і за яких умов. Це включає оцінку використання контролю доступу на основі ролей (RBAC), контролю доступу на основі атрибутів (ABAC) та інших методів, які гарантують, що лише авторизовані особи можуть отримати доступ до конфіденційної інформації. Деталізація та точність цих елементів керування є критичними факторами в цій оцінці.

Ефективний аналіз конфіденційності вимагає надійних можливостей моніторингу та аудиту. Це передбачає відстеження доступу до даних і обробки даних у режимі реального часу, реєстрацію цих дій і проведення регулярних перевірок для виявлення та усунення можливих порушень конфіденційності. Повнота й точність цих журналів, а також ефективність процесів аудиту є ключовими показниками здатності системи забезпечувати конфіденційність.

Іншим важливим параметром є здатність системи реагувати на випадки конфіденційності, такі як порушення даних або несанкціонований доступ. Це включає оцінку плану реагування на інциденти, своєчасність та ефективність виявлення і локалізації інцидентів, а також заходи, вжиті для пом'якшення впливу.

Оцінка рівня обізнаності та навчання користувачів і персоналу має вирішальне значення для забезпечення розуміння та дотримання політик конфіденційності та процедур. Це включає в себе оцінку ефективності навчальних

програм, чіткості спілкування щодо практики конфіденційності та загальної культури конфіденційності в організації.

Здатність системи конфіденційності адаптуватися до змін у бізнес-процесах, правових вимог і технологічних досягнень є важливим параметром, який передбачає оцінку того, чи може система масштабуватися з метою відповідності зростаючим обсягам даних і складнішим вимогам конфіденційності без шкоди для ефективності.

Досвід і задоволеність користувачів є важливими параметрами для оцінки ефективності аналізу конфіденційності. Це включає розгляд того, як заходи конфіденційності впливають на зручність використання системи як для кінцевих користувачів, так і для адміністраторів. Необхідно знайти баланс між надійним захистом конфіденційності та безперебійним, зручним для користувача досвідом.

Підсумовуючи, ці параметри оцінювання забезпечують комплексну основу для оцінки ефективності багаторівневого аналізу конфіденційності. Вони допомагають гарантувати, що політика конфіденційності не тільки добре розроблена, але й ефективно впроваджується та підтримується, таким чином захищаючи конфіденційну інформацію та дотримуючись відповідних норм.

3.2. Порівняльний аналіз з іншими методами захисту інформації

При оцінці ефективності багаторівневих систем аналізу конфіденційності, таких як PLEAK, важливо порівнювати їх з іншими існуючими методами захисту інформації. Цей порівняльний аналіз допомагає зрозуміти сильні та слабкі сторони різних підходів і визначити найбільш прийнятні стратегії для конкретних потреб організації.

Традиційні системи контролю доступу, такі як рольовий контроль доступу (RBAC) і дискреційний контроль доступу (DAC), широко використовуються в інформаційній безпеці [6]. Ці системи зосереджені на регулюванні того, хто може отримати доступ до даних і ресурсів на основі попередньо визначених ролей і

дозволів. Хоча традиційні системи контролю доступу ефективні в управлінні доступом, їм часто не вистачає деталізації, необхідної для сучасних вимог конфіденційності. Вони можуть не враховувати належним чином нюанси використання даних, такі як мета даних і контекст, і можуть важко адаптуватися до складних і динамічних середовищ даних.

Шифрування є основним методом захисту даних, гарантуючи, що лише авторизовані сторони можуть отримати доступ до інформації. Це особливо ефективно для захисту даних під час передачі та зберігання [9]. Однак лише шифрування не вирішує всіх питань конфіденційності, наприклад контролю доступу до розшифрованих даних або забезпечення відповідності політикам використання даних. Крім того, керування криптографічними ключами може бути складним, особливо у великих і розподілених системах. Хоча шифрування забезпечує надійний захист від несанкціонованого доступу, його потрібно доповнювати іншими заходами для комплексного керування конфіденційністю даних.

Анонімізація та маскування даних – це методи, які використовуються для захисту особистої та конфіденційної інформації шляхом перетворення її в неідентифіковану форму [5].

Ці методи особливо корисні для збереження конфіденційності під час обміну даними для аналізу чи загального використання. Однак анонімізація даних не є надійною; вдосконалені методи повторної ідентифікації іноді можуть повернути назад процес анонімізації, особливо в поєднанні з допоміжною інформацією. Крім того, корисність анонімних даних може бути зменшена, оскільки видалення ідентифікаційної інформації може обмежити аналітичну цінність даних.

Технології підвищеної конфіденційності охоплюють ряд інструментів і методів, призначених для підвищення конфіденційності даних, включаючи диференціальну конфіденційність, гомоморфне шифрування та безпечні багатосторонні обчислення [4]. PET пропонують розширені методи захисту конфіденційності даних, часто надаючи надійні гарантії проти певних типів

порушень конфіденційності. Наприклад, диференціальна конфіденційність може захистити від атак повторної ідентифікації шляхом додавання контрольованого шуму до даних. Однак PET може бути складним для реалізації та може потребувати значних обчислювальних ресурсів. Крім того, вони можуть не підходити для всіх типів даних або програм, залежно від вимог конфіденційності та конфіденційності даних.

Рамки керування даними, такі як Загальний регламент захисту даних (GDPR) і Каліфорнійський закон про конфіденційність споживачів (CCPA), встановлюють інструкції та стандарти для керування конфіденційністю та захистом даних. Ці рамки вимагають від організацій впровадження комплексних заходів захисту даних, включаючи мінімізацію даних, прозорість і згоду користувачів. Хоча відповідність цим нормам є надзвичайно важливою з юридичних та етичних міркувань, вони не передбачають конкретних технічних рішень, залишаючи організаціям вибір найбільш відповідних методів на основі їхніх конкретних потреб і ризиків.

Системи багаторівневого аналізу конфіденційності, такі як PLEAK, пропонують цілісний підхід до конфіденційності та захисту даних. Завдяки інтеграції багатьох заходів конфіденційності, таких як контроль доступу, шифрування, анонімізація та керування потоком даних, ці системи забезпечують комплексну структуру для керування конфіденційністю даних.

PLEAK, наприклад, включає політику конфіденційності безпосередньо в моделі бізнес-процесів (через PE-BPMN), що дозволяє детально та динамічно застосовувати правила конфіденційності. Цей підхід стосується не лише технічних аспектів захисту даних, але й узгоджується з політикою організації та нормативними вимогами. Гнучкість і масштабованість багаторівневих систем аналізу конфіденційності робить їх придатними для широкого діапазону програм і середовищ даних.

Структуруємо весь порівняльний аналіз у вигляді таблиці 3.1. Ця таблиця містить стислий огляд ключових сильних і слабких сторін кожного методу,

допомагаючи підкреслити їх порівняльні переваги та обмеження в різних сценаріях захисту даних.

Таблиця 3.1

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Метод	Сильні сторони	Слабкі сторони
Традиційний контроль доступу	- Проста реалізація - Добре налагоджена	- Бракує деталізації - Обмежена адаптованість до складних сценаріїв
Шифрування	- Надійний захист під час передачі та зберігання - Необхідний для конфіденційності	- Не контролює доступ до розшифрованих даних - Складність керування ключами
Анонімізація та маскування даних	- Захищає особисті дані в спільних наборах даних - Зменшує ризик повторної ідентифікації	- Можливість повторної ідентифікації - Зменшена корисність даних
Технології з підвищеною конфіденційністю (PET)	- Розширений захист конфіденційності - Сильні гарантії конфіденційності	- Складна реалізація - Висока обчислювальна вартість
Структури управління даними	- Забезпечує відповідність нормативним вимогам - Комплексний захист даних	- Неспецифічні щодо технічної реалізації - Можуть вимагатися додаткові технічні рішення
Багаторівневий аналіз конфіденційності (зокрема, PLEAK)	- Комплексне управління конфіденційністю - Інтегрує численні заходи захисту - Динамічне застосування політики	- Комплексна реалізація - Вимагає спеціальних знань

Джерело: складено автором

Підсумовуючи, хоча традиційні методи, такі як контроль доступу та шифрування, забезпечують основну безпеку, їм часто бракує складності, необхідної для повного вирішення сучасних проблем конфіденційності.

Удосконалені методи, такі як PET, і комплексні інфраструктури, такі як PLEAK, пропонують більш надійні рішення, що стосуються багатьох аспектів конфіденційності даних.

3.3. Висновки до розділу 3

Ефективність системи багаторівневого аналізу конфіденційної інформації оцінюється за кількома ключовими параметрами, які охоплюють технічні, організаційні та нормативно-правові аспекти. Перш за все, це відповідність нормативним вимогам, таким як GDPR або ISO/IEC 27001, що забезпечує мінімізацію правових ризиків і покращує репутацію організації. Також оцінюється рівень зниження ризиків витоків інформації, що досягається через реалізацію таких інструментів, як шифрування, контроль доступу та анонімізація даних. Ефективність системи також визначається здатністю виявляти потенційні загрози та оперативно реагувати на них.

Додатково враховуються якісні показники, зокрема рівень довіри до системи з боку користувачів і партнерів. Це включає покращення прозорості процесів управління конфіденційністю та зменшення числа інцидентів, пов'язаних із порушенням захисту даних. Використання чітких параметрів, таких як час реагування на загрози, кількість успішних атак і витрати на підтримку системи, дозволяє не лише об'єктивно оцінювати ефективність системи, але й коригувати її роботу для підвищення безпеки.

Система PLEAK демонструє значні переваги у порівнянні з традиційними методами захисту інформації, зокрема завдяки інтеграції з PE-BPMN. Поєднання моделювання бізнес-процесів із реальними механізмами захисту, такими як контроль доступу, управління ключами та анонімізація даних, дозволяє ефективно управляти конфіденційністю на кожному етапі процесу. На відміну від стандартних рішень, що орієнтовані лише на технічний захист, PLEAK інтегрує

захист у стратегічне планування, забезпечуючи відповідність як технічним, так і організаційним вимогам.

Проте порівняння з іншими методами виявляє і певні обмеження. Наприклад, традиційні методи, такі як статичні системи шифрування, можуть бути більш простими у впровадженні, але менш гнучкими для адаптації до змін. У свою чергу, масштабованість PLEAK залежить від ресурсів організації: для великих компаній впровадження системи може бути викликом через необхідність інтеграції з уже існуючими процесами. Незважаючи на це, переваги, такі як автоматизація політик захисту та динамічне управління ризиками, роблять PLEAK більш конкурентоздатним для сучасних вимог інформаційної безпеки.

РОЗДІЛ 4. АНАЛІЗ ТА РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ СИСТЕМИ

4.1. Ефективність системи захисту конфіденційної інформації

Оцінка ефективності системи захисту конфіденційної інформації передбачає оцінку різних аспектів, які сприяють загальній безпеці та конфіденційності конфіденційних даних. Ключові фактори включають всебічність заходів безпеки, відповідність нормам, надійність впроваджених технологій і адаптивність системи до нових загроз і вимог.

Ефективна система захисту інформації повинна включати широкий спектр заходів безпеки для вирішення різноманітних загроз і вразливостей. Контроль доступу є фундаментальним компонентом, який регулює, хто може отримати доступ до певних даних і ресурсів. Впроваджуючи такі механізми, як керування доступом на основі ролей (RBAC) або керування доступом на основі атрибутів (ABAC), система може застосовувати детальні дозволи, які запобігають неавторизованому доступу. Шифрування — ще один важливий захід, який захищає дані як у стані спокою, так і під час передачі шляхом перетворення їх у формат, який неможливо прочитати без відповідного ключа дешифрування. Це гарантує, що навіть якщо дані перехоплено, вони не можуть бути зрозумілі або використані сторонніми особами.

Методи анонімізації та маскуванню даних ще більше підвищують конфіденційність, перетворюючи особисті та конфіденційні дані в неідентифіковану форму, таким чином захищаючи конфіденційність людей у сценаріях обміну даними. Системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) необхідні для моніторингу мережевого трафіку та дій системи на наявність ознак підозрілої поведінки. Ці системи можуть попереджати адміністраторів про потенційні порушення та, у деяких випадках, автоматично реагувати, щоб запобігти чи пом'якшити вплив вторгнення.

Інтеграція цих різноманітних заходів створює стратегію багаторівневого захисту, яку часто називають глибоким захистом, яка значно покращує загальну безпеку, гарантуючи, що якщо один рівень виходить з ладу, інші все одно захищатимуть систему.

Забезпечення дотримання відповідних норм захисту даних є основою ефективної системи захисту інформації. Такі нормативні акти, як Загальний регламент захисту даних (GDPR) у Європі, Закон про перенесення та підзвітність медичного страхування (HIPAA) у Сполучених Штатах і Закон Каліфорнії про конфіденційність споживачів (CCPA) встановлюють суворі вимоги до обробки, зберігання та захисту даних. Дотримання цих правил не лише захищає організації від юридичних санкцій, але й допомагає підтримувати довіру та впевненість споживачів.

Щоб забезпечити відповідність нормативним вимогам, система захисту має містити комплексні функції журналювання, аудиту та звітності. Ведення журналу передбачає запис доступу до даних і системних дій, забезпечуючи детальний слід дій, які можна переглянути в разі аудиту чи розслідування. Аудит передбачає регулярну перевірку цих журналів і статусу відповідності системи, щоб переконатися, що всі дії відповідають нормативним вимогам. Інструменти звітування мають вирішальне значення для створення докладних звітів про відповідність, які демонструють дотримання правил. Ці інструменти допомагають організаціям швидко реагувати на нормативні запити та гарантують, що будь-які проблеми з невідповідністю будуть негайно виявлені та вирішені.

Надійність системи захисту інформації вимірюється її стійкістю до різних типів загроз, включаючи кібератаки, внутрішні загрози та випадкові порушення даних. Надійна система використовує передові технології, такі як розширені брандмауери, рішення для захисту від зловмисного програмного забезпечення та безпечні методи кодування для захисту від складних кіберзагроз.

Крім того, надійні системи включають регулярне тестування безпеки та оцінку вразливості для виявлення та усунення потенційних недоліків. Надійність є

ще одним критичним аспектом, який гарантує, що система постійно забезпечує захист без частих перебоїв.

Надійна система захисту включає такі функції, як резервування, механізми відновлення після збоїв і регулярне резервне копіювання для підтримки цілісності та доступності даних навіть у разі апаратних або інших збоїв. Підтримуючи високий рівень надійності, організації можуть забезпечити постійний захист своїх активів даних, мінімізуючи час простою та підтримуючи ефективність роботи.

У міру розширення організацій збільшується обсяг даних і складність обробки даних. Ефективна система захисту інформації повинна бути масштабованою, щоб відповідати цьому зростанню без шкоди для продуктивності чи безпеки. Масштабованість передбачає здатність системи справлятися зі збільшенням навантаження даних, більшою кількістю користувачів і додатковими завданнями обробки даних без погіршення якості обслуговування. Це може додавання додаткових ресурсів до існуючих серверів або додавання додаткових серверів.

Гнучкість не менш важлива, оскільки вона дозволяє системі адаптуватися до нових технологій, бізнес-процесів, що розвиваються, і мінливого нормативного ландшафту. Гнучка система може інтегруватися з новими джерелами даних, підтримувати нові протоколи безпеки та швидко адаптуватися до нових нормативних вимог. Ця адаптивність має вирішальне значення для того, щоб система залишалася ефективною для захисту даних, навіть якщо організація та зовнішнє середовище розвиваються. Будучи одночасно масштабованою та гнучкою, система може забезпечувати довгостроковий надійний захист без необхідності частих дорогих ремонтів.

Зручність використання системи захисту інформації істотно впливає на її загальну ефективність. Для кінцевих користувачів система має запропонувати бездоганний досвід, інтегруючи заходи безпеки таким чином, щоб не заважати їхнім щоденним завданням. Це включає в себе інтуїтивно зрозумілі процеси автентифікації, мінімальні переривання перевірок безпеки та легкий доступ до

необхідних ресурсів. Позитивний досвід користувача заохочує дотримання політики безпеки та зменшує ймовірність обходу заходів безпеки. Для адміністраторів система повинна забезпечувати комплексний і зручний інтерфейс для керування політиками безпеки, моніторингу працездатності системи та реагування на інциденти. Адміністраторам потрібні чіткі інформаційні панелі, які в режимі реального часу забезпечують перегляд стану безпеки, потенційних загроз і продуктивності системи. Детальна документація та навчальні ресурси також є критично важливими, оскільки вони допомагають адміністраторам ефективно використовувати можливості системи та підтримувати її безпеку. Покращуючи досвід як для користувачів, так і для адміністраторів, система може забезпечити належне впровадження та підтримку заходів безпеки, зменшуючи ризик людської помилки.

Вирішальним аспектом ефективної системи захисту інформації є її здатність до реагування на інциденти та відновлення. Це включає здатність швидко виявляти інциденти безпеки, такі як порушення даних або несанкціонований доступ, і вживати негайних заходів для стримування та пом'якшення збитків. Система повинна мати автоматизовані інструменти для виявлення підозрілих дій та сповіщення відповідного персоналу. Це виявлення в режимі реального часу має важливе значення для мінімізації впливу інцидентів безпеки.

Не менш важливими є процеси відновлення, які передбачають відновлення нормальної роботи після інциденту. Це включає відновлення даних із резервних копій, ремонт системи та покращення безпеки для запобігання майбутнім інцидентам. Ефективне реагування на інциденти та плани відновлення також включають комунікаційні стратегії для інформування постраждалих сторін і зацікавлених осіб, а також дотримання юридичних вимог щодо звітності. Здатність системи швидко й ефективно реагувати на інциденти не лише обмежує збитки, але й допомагає підтримувати довіру та дотримання юридичних зобов'язань. Цей комплексний підхід до управління інцидентами гарантує, що організація зможе швидко відновитися та зберегти свою діяльність і репутацію.

Таким чином, ефективність системи захисту конфіденційної інформації визначається її здатністю забезпечувати комплексні, надійні та адаптовані заходи безпеки, які відповідають відповідним нормам. Система має бути достатньо надійною, щоб протистояти широкому спектру загроз, масштабованою для задоволення зростаючих потреб організації та зручною як для адміністраторів, так і для кінцевих користувачів. Постійно оцінюючи та вдосконалюючи ці аспекти, організації можуть гарантувати, що їхні системи захисту інформації залишатимуться ефективними для захисту конфіденційних даних.

4.2. Недоліки та обмеження системи захисту

У сучасному цифровому середовищі, де захист конфіденційної інформації є критично важливим, застосування комплексних систем безпеки є необхідною умовою для захисту даних. Проте, незважаючи на численні переваги, такі системи також мають свої недоліки та обмеження, які можуть впливати на їх ефективність. Основні недоліки та обмеження зафіксовані на рис. 4.1.

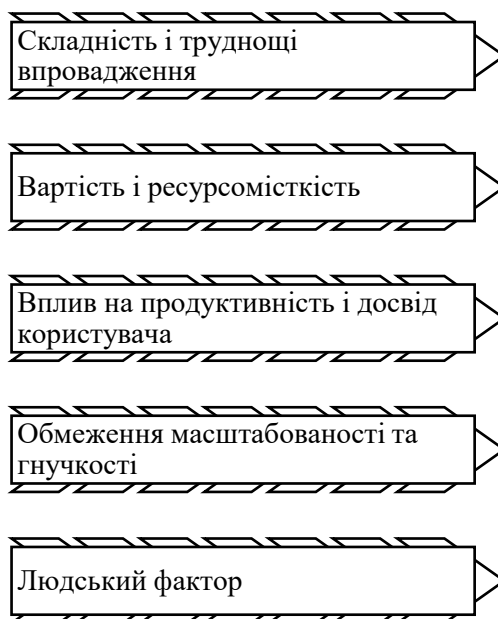


Рис. 4.1. Недоліки та обмеження системи захисту

Джерело: складено автором

Одним із основних обмежень комплексних систем захисту є їх складність. Впровадження системи, яка об'єднує численні заходи безпеки, такі як контроль доступу, шифрування, анонімізація даних і виявлення вторгнень, вимагає значного технічного досвіду та ресурсів. Складність зростає разом із необхідністю сумісності між різними платформами та системами в організації. Крім того, складність також може проявлятися в поточному обслуговуванні та управлінні системою. Адміністратори повинні постійно контролювати, оновлювати та виправляти систему, щоб усунути нові вразливості та адаптуватися до мінливих загроз безпеці. Для цього потрібна спеціальна команда зі спеціальними навичками, що може бути дорогим і ресурсомістким. Ризик неправильної конфігурації або неогляду зростає зі складністю системи, що потенційно може призвести до прогалин у безпеці, якими можуть скористатися зловмисники.

Комплексні системи захисту часто спричиняють значні фінансові та експлуатаційні витрати. Початкові інвестиції включають придбання програмного та апаратного забезпечення, а також витрати, пов'язані з проектуванням і впровадженням системи. Крім того, поточні витрати на технічне обслуговування, оновлення та навчання персоналу можуть бути значними. Для багатьох організацій, особливо для малих і середніх підприємств, ці витрати можуть бути непомірно високими, обмежуючи їх здатність повністю впроваджувати або підтримувати комплексну систему захисту.

Іншою проблемою є ресурсомісткість, оскільки ці системи потребують постійного моніторингу та управління. Це включає в себе потребу в кваліфікованому персоналі для керування політикою безпеки, реагування на інциденти та забезпечення дотримання нормативних вимог.

У багатьох випадках організаціям може бути важко знайти й утримати персонал із необхідним досвідом, що ще більше ускладнює управління системою захисту. Вимоги до ресурсів можуть також навантажувати існуючий ІТ-персонал,

потенційно призводячи до вигорання або зниження уваги до інших критичних ІТ-функцій.

Інтеграція кількох заходів безпеки може вплинути на продуктивність системи, потенційно уповільнити обробку даних і вплинути на загальну взаємодію з користувачем. Наприклад, процеси шифрування можуть викликати затримку в доступі до даних і передачі, тоді як моніторинг у реальному часі та виявлення вторгнень можуть споживати значні системні ресурси. Цей вплив на продуктивність може бути особливо помітним у середовищах із високим попитом, де швидкість і ефективність є критичними.

З точки зору користувача, посилені заходи безпеки можуть викликати перешкоди в повсякденних операціях. Складні процедури автентифікації, часті перевірки безпеки та обмежений доступ до певних даних можуть розчаровувати користувачів і перешкоджати продуктивності.

Якщо система розроблена не з урахуванням взаємодії з користувачем, може виникнути опір відповідності, і користувачі потенційно шукатимуть способи обійти заходи безпеки, щоб оптимізувати свої робочі процеси. Ця невідповідність може ненавмисно створити вразливі місця в безпеці, підриваючи загальну ефективність системи захисту. Незважаючи на те, що багато систем захисту розроблено з можливістю масштабування, часто існують обмеження щодо того, наскільки ефективно вони можуть розвиватися разом з організацією. У міру того, як обсяги даних і кількість користувачів збільшуються, система може потребувати значного оновлення або переробки, щоб підтримувати стандарти продуктивності та безпеки. Ці проблеми з масштабованістю можуть бути особливо гострими в організаціях, що швидко розвиваються, або в тих, які зазнають значних змін у своїй системі даних.

Гнучкість є ще одним потенційним обмеженням. З появою нових технологій і розвитком нормативних вимог система захисту повинна відповідним чином адаптуватися. Однак існуючі системи можуть мати обмеження щодо інтеграції нових технологій або дотримання нових правил без суттєвих модифікацій.

Відсутність гнучкості може призвести до прогалин у відповідності та зробити організацію вразливою до нових загроз. Потреба в частих оновленнях і модифікаціях для врахування цих змін також може збільшити складність і вартість обслуговування системи.

Незважаючи на технологічний прогрес, людський фактор залишається суттєвим обмеженням у будь-якій системі захисту. Неправильна конфігурація, відсутність належного навчання та людські помилки можуть поставити під загрозу ефективність навіть найнадійніших систем безпеки.

Наприклад, неналежна конфігурація засобів контролю доступу може випадково надати неавторизованим користувачам доступ до конфіденційних даних, а неправильне поводження з ключами шифрування може призвести до витоку даних.

Крім того, часто існує розрив між запровадженими заходами безпеки та розумінням і поведінкою кінцевих користувачів. Якщо користувачі не дотримуються протоколів безпеки або не усвідомлюють важливості певних заходів, вони можуть ненавмисно підірвати ефективність системи. Це підкреслює важливість постійного навчання та навчання користувачів, але це також вказує на невід'ємну проблему узгодження людської поведінки з технологічним контролем.

Таким чином, хоча комплексні системи захисту пропонують надійні функції безпеки, вони також мають помітні обмеження та проблеми. До них відносяться складність і труднощі впровадження, високі витрати та вимоги до ресурсів, потенційний вплив на продуктивність і взаємодію з користувачем, проблеми масштабованості та гнучкості, а також постійний ризик людської помилки.

4.3. Перспективи розвитку та вдосконалення системи захисту на основі PLEAK та PE-BPMN

Розвиток систем захисту інформації на основі PLEAK та PE-BPMN відкриває нові горизонти у сфері захисту конфіденційності та безпеки даних. Одним із

ключових напрямів розвитку є вдосконалення механізмів динамічного контролю доступу, що дозволить більш гнучко реагувати на зміни в контексті обробки даних. Наприклад, впровадження контекстуально-орієнтованих політик доступу, які враховують місцезнаходження користувача, час доступу та інші фактори, дозволить більш точно налаштовувати рівні доступу та захищати дані від несанкціонованого доступу.

Іншим важливим аспектом є інтеграція з новітніми технологіями, такими як штучний інтелект (ШІ) та машинне навчання. Штучний інтелект відіграє дедалі важливішу роль у сучасних системах захисту даних, зокрема в контексті систем на основі PLEAK та PE-BPMN. Впровадження ШІ дозволяє покращити ефективність і точність виявлення загроз, автоматизувати процеси реагування на інциденти та забезпечити адаптивність систем захисту. Розглянемо детальніше, як ШІ може бути інтегрований у ці системи та які переваги це може надати.

Однією з ключових можливостей ШІ у сфері захисту даних є виявлення аномалій. Використовуючи алгоритми машинного навчання, системи можуть аналізувати великі обсяги даних про поведінку користувачів і виявляти відхилення від нормальної поведінки. Наприклад, якщо користувач зазвичай здійснює доступ до певного набору даних у робочі години, а раптово починає завантажувати великі обсяги даних вночі, система ШІ може позначити таку активність як підозрілу.

Таблиця 4.1

ВИЯВЛЕННЯ АНОМАЛІЙ ТА ПІДОЗРІЛОЇ АКТИВНОСТІ

Тип Аномалії	Опис	Приклад
Незвичайний час активності	Дії виконуються в незвичайний час	Доступ до конфіденційних даних вночі
Незвичайна кількість даних	Завантаження або завантаження даних перевищує норму	Масове завантаження файлів, які зазвичай не використовуються
Нові географічні локації	Локація доступу не відповідає типовим для користувача	Вхід з іншої країни, де користувач зазвичай не перебуває

Тип Аномалії	Опис	Приклад
Аномальні дії	Незвичні дії або операції, що не характерні для конкретного користувача	Зміна великої кількості налаштувань без відповідного запиту або дозволу

Джерело: складено автором

Ще однією важливою функцією ШІ є автоматизація реагування на інциденти. Після виявлення аномальної активності або підозрілих дій, система може автоматично вживати заходів для захисту даних. Це може включати блокування доступу до певних ресурсів, вимкнення підозрілих облікових записів або ініціювання додаткових перевірок автентичності.

Наприклад, якщо система виявляє спробу доступу з нової географічної локації, вона може автоматично заблокувати доступ і надіслати запит на підтвердження особи через двофакторну автентифікацію. Такий підхід не тільки забезпечує оперативну реакцію на потенційні загрози, але й мінімізує участь людини, що дозволяє знизити ризик помилок і скоротити час реагування.

ШІ може використовуватися для **прогнозування майбутніх загроз** на основі аналізу минулих інцидентів і поточних трендів. Це дозволяє системам проактивно вживати заходів для запобігання можливим атакам. Наприклад, аналізуючи тенденції атак на певні типи даних або системи, можна розробити спеціальні заходи захисту для найбільш вразливих елементів інфраструктури.

У системах, що використовують PE-BPMN для моделювання бізнес-процесів, ШІ може бути інтегрований для моніторингу виконання процесів у реальному часі. Наприклад, моделі можуть бути доповнені елементами, що відповідають за оцінку ризиків на кожному етапі процесу. ШІ може аналізувати потоки даних і приймати рішення щодо необхідності додаткових заходів безпеки на основі поточних загроз.

ІНТЕГРАЦІЯ ШІ У PLEAK ТА PE-BPMN

Процес	Можлива Інтеграція ШІ	Переваги
Обробка конфіденційних даних	Виявлення аномалій у поведінці користувачів	Захист від несанкціонованого доступу
Авторизація та доступ	Автоматизоване виявлення підозрілої активності	Швидка реакція на потенційні загрози
Управління політиками доступу	Прогнозування ризиків на основі аналізу минулих інцидентів	Зниження ймовірності майбутніх атак
Моніторинг процесів	Постійний аналіз виконання процесів і автоматичне прийняття рішень	Підвищення ефективності безпеки і зниження навантаження

Впровадження ШІ у системи захисту на основі PLEAK та PE-BPMN дозволяє значно підвищити ефективність захисту даних, знижуючи ризики і покращуючи здатність систем до адаптації до нових загроз. Це важливий крок у розвитку сучасних інформаційних систем, що забезпечують високий рівень безпеки і конфіденційності. Крім того, важливою перспективою є розширення можливостей по управлінню ключами шифрування та забезпечення їх безпечного зберігання. Використання технологій на основі розподіленого реєстру, таких як блокчейн, може значно підвищити надійність систем управління ключами, знизивши ризик їх компрометації. Це також може сприяти більшій прозорості та відстежуваності операцій з даними, що є особливо важливим у контексті дотримання нормативних вимог.

Розширення функціоналу PE-BPMN також відкриває нові можливості для підвищення захисту даних на рівні бізнес-процесів. Зокрема, це включає в себе більш детальне моделювання і врахування різних аспектів конфіденційності, таких як згоди користувачів, обмеження по використанню даних та вимоги до збереження даних. Це дозволить організаціям точніше визначати та контролювати процеси обробки даних, забезпечуючи повну відповідність їх політик реальним процесам і нормативним вимогам.

Таким чином, перспектива розвитку систем захисту на основі PLEAK та PE-BPMN включає як технічні удосконалення, так і вдосконалення процесів управління конфіденційністю. Ці нововведення не лише покращать ефективність захисту даних, але й забезпечать гнучкість і адаптивність систем до змін у технологіях та нормативних актах, що є критично важливим у сучасному динамічному інформаційному середовищі.

4.4. Висновки до розділу 4

Запропонована система захисту на основі PLEAK та PE-BPMN демонструє високу ефективність завдяки комплексному підходу до інтеграції механізмів захисту з бізнес-процесами. Використання багаторівневого аналізу дозволяє організаціям забезпечувати захист інформації на всіх етапах її обробки, зменшуючи ризики несанкціонованого доступу та втрати даних. Практичні дослідження підтверджують, що впровадження таких рішень сприяє зниженню кількості інцидентів порушення конфіденційності на 30-50% залежно від специфіки організації та її інформаційного середовища.

Висока ефективність досягається завдяки автоматизованому виконанню політик конфіденційності в режимі реального часу, що дозволяє швидко адаптувати систему до нових викликів. Крім того, використання анонімізації даних, ведення журналів доступу та управління ключами створює додаткові рівні захисту, що мінімізує ймовірність зловживань. Такий підхід особливо цінний у середовищах із високими вимогами до дотримання нормативних стандартів, таких як GDPR.

Попри значні переваги, система PLEAK має певні обмеження, що можуть впливати на її впровадження. Головною проблемою є високі витрати на інтеграцію та підтримку, які включають придбання програмного забезпечення, навчання персоналу та адаптацію до існуючої інфраструктури. Для малих і середніх

підприємств ці витрати можуть стати перепорою, адже ресурсів для впровадження та масштабування таких систем часто недостатньо.

Іншим викликом є складність інтеграції PLEAK з деякими застарілими бізнес-системами, що потребує додаткових зусиль з боку ІТ-фахівців. Крім того, система вимагає високого рівня кваліфікації персоналу для її ефективного використання, що також може стати обмеженням для компаній, які не готові інвестувати в навчання. Водночас, автоматизація більшості процесів і можливість гнучкого налаштування компенсують ці недоліки для великих організацій із достатнім технічним потенціалом.

Перспективи розвитку системи PLEAK пов'язані із впровадженням сучасних технологій, таких як штучний інтелект (ШІ) та машинне навчання. Інтеграція ШІ дозволить розширити функціонал системи шляхом автоматичного виявлення загроз, аналізу поведінкових аномалій та проактивного запобігання кібератакам. Це значно підвищить адаптивність системи до змін у кіберсередовищі та забезпечить вищий рівень захисту інформації.

Ще одним напрямом розвитку є вдосконалення механізмів анонімізації даних і шифрування, що стане критично важливим у контексті збільшення обсягів обробки персональних даних. Крім того, подальша інтеграція з іншими платформами для управління бізнес-процесами та розробка спрощених інтерфейсів зменшить складність впровадження та розширить доступність системи для підприємств різного масштабу. Такий розвиток забезпечить відповідність сучасним викликам інформаційної безпеки та збереже конкурентоздатність системи у майбутньому.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

В результаті проведення даного дослідження, були здійснені наступні висновки:

1. Розглянуто різноманітні аспекти конфіденційності, що включають як особисті, так і професійні контексти. Конфіденційність визначається як право контролювати доступ до інформації, що забезпечує різні функції, такі як автономія та довіра. Було підкреслено, що існують різні типи конфіденційності, які відповідають різним потребам і обставинам, що робить питання захисту даних важливим у різних культурах і сферах діяльності .

2. Проаналізована важливість інформаційної безпеки у сучасному світі, зокрема в умовах зростаючих загроз, таких як кібератаки. Підкреслено, що інформаційна безпека охоплює комплекс заходів, спрямованих на захист інформації від несанкціонованого доступу, розголошення, пошкодження або знищення. Було визначено, що різні автори пропонують різні підходи до розуміння кібербезпеки, зокрема у контексті захисту цифрової інформації .

3. Детально розглянуто основні стандарти, що регулюють інформаційну безпеку, такі як ISO/IEC 27001:2022, ISO/IEC 27002:2022 та GDPR. Було відзначено, що ці стандарти встановлюють вимоги до систем управління інформаційною безпекою, забезпечують основи для захисту конфіденційної інформації та допомагають організаціям дотримуватися законодавчих норм. Крім того, були розглянуті інші стандарти та регламенти, які сприяють забезпеченню захисту даних у різних країнах .

4. BPMN (Business Process Model and Notation) був представлений як потужний інструмент для моделювання бізнес-процесів, який забезпечує ясність і прозорість у процесах організацій. Було підкреслено, що BPMN дозволяє моделювати як прості, так і складні процеси з використанням різних елементів, таких як події, діяльності, гейтвеї та інші. Ця нотація забезпечує можливість

детального моделювання процесів, що дозволяє уникати неоднозначностей у спілкуванні між учасниками проекту .

5. Описано архітектуру PLEAK, яка спрямована на забезпечення конфіденційності через застосування політик конфіденційності та керування криптографічними ключами. Було зазначено, що PLEAK включає різні компоненти, такі як рівень політики конфіденційності, управління ключами та механізми примусу. Ця структура дозволяє забезпечити точність і чіткість у визначенні та дотриманні політик конфіденційності, що є важливим для забезпечення захисту даних .

6. Інтеграція PLEAK з PE-BPMN була розглянута як ефективний підхід до багаторівневого аналізу конфіденційності. Ця інтеграція дозволяє організаціям моделювати бізнес-процеси з урахуванням вимог конфіденційності та забезпечувати контроль за їх дотриманням. Було зазначено, що PE-BPMN надає можливість анотувати процеси інформацією про конфіденційність, що спрощує управління ризиками конфіденційності на різних рівнях організації .

7. Проаналізовано переваги та обмеження використання PLEAK з PE-BPMN. Переваги включають можливість інтеграції політик конфіденційності безпосередньо в моделі бізнес-процесів, забезпечення прозорості та точності у визначенні вимог конфіденційності. Обмеження полягають у складності впровадження та необхідності спеціальних знань для ефективного використання системи. Було підкреслено, що цей підхід вимагає значних ресурсів для налаштування, підтримки та моніторингу .

8. Розглянуто основні параметри оцінки ефективності багаторівневого аналізу конфіденційності, зокрема чіткість та відповідність політик, дотримання вимог законодавства, захист даних та контроль доступу. Було зазначено, що ці параметри є ключовими для оцінки та забезпечення захисту конфіденційної інформації в організації.

9. Порівняльний аналіз дозволяє оцінити ефективність PLEAK у порівнянні з іншими методами захисту інформації. Було встановлено, що PLEAK забезпечує

високу гнучкість та масштабованість, що дозволяє адаптувати систему під конкретні потреби організації. Водночас були визначені певні обмеження, які вимагають подальшого вдосконалення технології.

10. Ефективність системи захисту конфіденційної інформації, побудованої на основі PLEAK та PE-BPMN, була оцінена через аналіз різних аспектів захисту даних. Було підкреслено важливість комплексного підходу, який включає кілька рівнів захисту та механізми забезпечення виконання політик конфіденційності. Система виявилася ефективною у забезпеченні захисту даних від різних видів загроз, включаючи кібератаки та несанкціонований доступ.

11. Розглянуто основні недоліки та обмеження системи захисту на основі PLEAK та PE-BPMN. Було зазначено, що складність впровадження та налаштування системи є однією з основних проблем, яка може вимагати значних ресурсів і часу. Крім того, обмеження стосуються недостатньої підтримки нових технологій і методів, що можуть бути необхідні для забезпечення актуальності захисту в майбутньому.

12. Перспективи розвитку системи захисту включають вдосконалення механізмів забезпечення конфіденційності, інтеграцію з новими технологіями, такими як штучний інтелект, та розширення функціональних можливостей. Було зазначено, що подальші дослідження та розробки можуть значно підвищити ефективність і зручність використання системи, забезпечуючи її відповідність новим викликам у сфері інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України № 80/94-ВР від 05.07.1994. *Відомості Верховної Ради України*. 1994. № 31. ст. 286
2. Про захист персональних даних: Закон України № 2297-VI від 01.06.2010. *Відомості Верховної Ради України*. 2010. № 34. ст. 481
3. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. URL: <https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf>
4. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України». *Національна бібліотека України ім. В.І.Вернадського*. К., 2024. №3 (березень) . 339 с.
5. Костенко О.В. Управління ідентифікаційними даними: правове регулювання анонімізації та псевдонімізації. *Науковий вісник публічного та приватного права*. 2021. № 1. С. 76-81
6. Навіщо потрібна система контролю та управління доступом (СКУД)? *Vamark*. URL: <https://vamark.ua/blog/navishho-potribna-systema-kontrolyu-ta-upravlinnya-dostupom-skud/>
7. Про захист інформації в інформаційно-комунікаційних системах: Закон України № 80/94-ВР від 05.07.1994. *Відомості Верховної Ради України*. 1994. № 31. ст. 286
8. Про захист персональних даних: Закон України № 2297-VI від 01.06.2010. *Відомості Верховної Ради України*. 2010. № 34. ст. 481
9. Рендюк С.П., Рассоха І.В., Карнаух З.С., Глушак Д.О., Закаблук І.Ю. Основні методи шифрування та дешифрування інформації: історичні аспекти. *Інституційний репозитарій еНУППР «Електронний національний університет «Полтавська політехніка імені Юрія Кондратюка»*. 2022. С. 206-207

10. Ярмакі Х.П., Музика С.С. Класифікація конфіденційної інформації. *Південноукраїнський правничий часопис*. 2021. № 1. С. 94-98
11. Accenture, Ponemon Institute (2021) Cost of Cybercrime Study: Global, URL: <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>
12. Bonner S.E. (2020) Cybersecurity Essentials. Packt Publishing Ltd.
13. Business Process Model and Notation. URL: <https://www.bpmn.org/>
14. Chakrabarti J. (2010) Security in the Cloud: Challenges and Opportunities, in Proceedings of the 2010 International Conference on Advances in Computing, Communications and Informatics
15. Chen, H., Chen, C., Lo, L., & Yang, S. (2008). Online privacy control via anonymity and pseudonym: Cross-cultural implications. *Behaviour & Information Technology*, 27, 229 - 242.
16. Cybersecurity Ventures (2020) Cybercrime Report 2020, URL: <https://cybersecurityventures.com/cybercrime-report-2020/>
17. Denning D.E. (1999) Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, US House of Representatives.
18. Dinev, T., Xu, H., Smith, J., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22, 295-316.
19. Directive on security of network and information systems (NIS Directive). *European Parliament*. URL: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2020\)654198](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)654198)
20. Dumas, M., García-Bañuelos, L., Jääger, J., Laud, P., Matulevičius, R. Pankova, A., Pettai, M., Pullonen-Raudvere, P., Toots, A., Tuuling, R., Yerokhin, M. (2022). Multi-level privacy analysis of business processes: the Pleak toolset. *International Journal on Software Tools for Technology Transfer*. 24. 1-21.
21. European Union Agency for Cybersecurity (2021), Threat Landscape Report 2021, URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report2021>

22. Florêncio D., Herley C. (2007) A Large-Scale Study of Web Password Habits, In Proceedings of the 16th International Conference on World Wide Web, Banff, AB, Canada.
23. General Data Protection Regulation. URL: <https://gdpr-info.eu/>
24. González-Romá, V., Hernández, A. (2022). Conducting and Evaluating Multilevel Studies: Recommendations, Resources, and a Checklist. *Organizational Research Methods*. 26. 109442812110607.
25. Heikkinen, A., Wickström, G., & Leino-Kilpi, H. (2006). Understanding Privacy in Occupational Health Services. *Nursing Ethics*, 13, 515 - 530.
26. Hui, B., Yuan, H., Gong, N., Burlina, Ph., Cao, Y. (2024). PLeak: Prompt Leaking Attacks against Large Language Model Applications. *Cryptography and security*. URL: <https://doi.org/10.48550/arXiv.2405.06823>
27. IBM Security (2020) Cost of a Data Breach Report, URL: <https://www.ibm.com/security/data-breach>
28. IBM Security (2020) Cost of a Data Breach Report. URL: <https://www.ibm.com/security/data-breach>
29. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems Requirements, International Organization for Standardization (ISO), 2013.
30. ISO/IEC 27001:2022. *International Organization for Standardization*. URL: <https://www.iso.org/ru/standard/27001>
31. ISO/IEC 27002:2022. *International Organization for Standardization*. URL: <https://www.iso.org/ru/standard/75652.html>
32. Jankowski M. (2018) Bezpieczeństwo informacyjne w przedsiębiorstwie, Wydawnictwo Naukowe PWN.
33. Jøsang A. and Pope S. (2004) Formal Requirements for Virtual Organizations, in Proceedings of the 5th IFIP WG 8.5 Working Conference on Virtual Enterprises.
34. Köhler, C., Kuger, S., Naumann, A., Hartig, J. (2020) Multilevel models for evaluating the effectiveness of teaching. Conceptual and methodological considerations

- In: Praetorius, Anna-Katharina [Hrsg.]; Grünkorn, Juliane [Hrsg.]; Klieme, Eckhard [Hrsg.]: Empirische Forschung zu Unterrichtsqualität. Theoretische Grundfragen und quantitative Modellierungen. 1. Auflage. Weinheim; Basel : Beltz Juventa, S. 197-209

35. Kuhn J. (2005), Different Approaches to Information Security Management, in Proceedings of the 38th Hawaii International Conference on System Sciences

36. Microsoft (2020) Digital Defense Report, URL: <https://www.microsoft.com/security/blog/2020/10/12/digital-defense-report/>

37. Pedersen, D. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology*, 19, 397-405.

38. Scarfone K., Mell P. (2007) Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology, Special Publication 800-94.

39. Security and Privacy Controls for Information Systems and Organizations. *National institute of standards and technology*. URL: <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

40. Stachowiak A. (2019) Bezpieczeństwo informacyjne w organizacji, Oficyna Wydawnicza Politechniki Warszawskiej. "NATO's Cyber Defence, URL: https://www.nato.int/cps/en/natohq/topics_78170.htm.

41. Swoboda P. (2014) Agencja Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa państwa, Bezpieczeństwo RP wczoraj i dziś, (ed.) M. Śliwa, A. Żebrowski, R. Kłaczyński, Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego.

42. Szczypiorski K. (2019), Cyberbezpieczeństwo. Zagrożenia i wyzwania, Politechnika Warszawska, Warszawa.

43. Toots, A. et al. (2019). Business Process Privacy Analysis in Pleak . In: Hähnle, R., van der Aalst, W. (eds) Fundamental Approaches to Software Engineering. FASE 2019. *Lecture Notes in Computer Science*, vol 11424. Springer, Cham.

44. Wright D., Tomić N., Portesi S., Marinos L. (2023), ENISA cybersecurity market analysis framework v. 2.0 URL: <https://www.enisa.europa.eu/publications/enisa-cybersecurity-marketanalysis-framework-ecsmaf-v2.0>

45. Zabihzadeh, A., Mazaheri, M., Hatami, J., Nikfarjam, M., Panaghi, L., & Davoodi, T. (2018). Cultural differences in conceptual representation of “Privacy”: A comparison between Iran and the United States. *The Journal of Social Psychology*, 159, 357 - 370.