ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТУ ІМЕНІ С.П.КОРОЛЬОВА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

здобувача вищої освіти ступеня «бакалавр» заочної форми навчання
за спеціальністю «Кібербезпека»

Тема: «МЕТОДИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВОМУ СЕРЕДОВИЩІ»

Виконавець: Валерій БЕРЕЗЮК

м. Житомир

2026

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПД — персональні дані

ПЗ — програмне забезпечення

ШПЗ — шкідливе програмне забезпечення

ІТ — інформаційні технології

КС — комп’ютерна система

ЗІ — захист інформації

ПК — персональний комп’ютер

ЕОМ — електронна обчислювальна машина

ІС — інформаційна система

НТІР — науково-технічні інформаційні ресурси

ЗМІ — засоби масової інформації

БД — база даних

ЗКЗІ — засоби криптографічного захисту інформації

ОС — операційна система

СІА — система ідентифікації та авторизації

RSA — Rivest-Shamir-Adleman — стандарт шифрування даних

ШПЗ — шкідливе програмне забезпечення

ВСТУП

Стрімкий розвиток інформаційних технологій та цифровізація практично всіх сфер суспільного життя зумовлюють постійне зростання обсягів інформації, що обробляється в електронному вигляді. Особливе місце серед цієї інформації займають персональні дані,(ПД) які є об’єктом збирання, зберігання, обробки та передачі в інформаційних системах державних установ, комерційних організацій і приватних сервісів. Активне використання мережі Інтернет, мобільних застосунків, соціальних мереж, хмарних обчислень та електронних сервісів суттєво підвищує зручність і швидкість доступу до інформації, проте одночасно створює нові загрози для її безпеки.

У цифровому середовищі ПД є одним із найбільш цінних інформаційних ресурсів і, відповідно, однією з основних цілей кіберзлочинців. Несанкціонований доступ, витоки інформації, фішингові атаки, використання шкідливого програмного забезпечення (ПЗ), атаки на вебзастосунки та хмарні платформи можуть призвести до порушення конфіденційності, цілісності та доступності ПД. Наслідками таких інцидентів є фінансові втрати, репутаційна шкода, порушення безперервності бізнес-процесів, а також порушення прав і свобод суб’єктів ПД .

З позицій кібербезпеки особливу увагу слід приділяти технічним і програмним аспектам захисту ПД . Недостатній рівень захищеності інформаційних систем, наявність вразливостей програмного забезпечення, помилки конфігурації, слабкі механізми автентифікації та контролю доступу значно підвищують ризик успішної реалізації кібератак. У зв’язку з цим актуальним є впровадження комплексного підходу до захисту ПД , який поєднує криптографічні методи, засоби керування доступом, моніторинг безпеки, резервне копіювання та реагування на інциденти інформаційної безпеки.

Метою дипломної роботи є розроблення та обґрунтування методики захисту ПД в інформаційних системах на основі сучасних підходів і технологій кібербезпеки.

РОЗДІЛ 1. ОБГРУНТУВАННЯ НЕОБХІДНОСТІ РОЗРОБЛЕННЯ МЕТОДИКИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВОМУ СЕРЕДОВИЩІ.

1.1 Аналіз сучасних загроз для інформаційних ресурсів систем та персональних даних.

У сучасних умовах цифрової трансформації суспільства інформація стає одним із ключових ресурсів розвитку держави, бізнесу та окремої особи. Особливе місце серед інформаційних ресурсів займають персональні дані, обробка яких здійснюється в інформаційних системах різного рівня складності. Масове використання мережі Інтернет, електронних сервісів, мобільних додатків і хмарних технологій суттєво підвищує ризики виникнення загроз інформаційній безпеці.

Сучасні загрози для персональних даних характеризуються високим рівнем динамічності та різноманітності. Однією з найбільш поширених загроз є несанкціонований доступ до інформаційних систем, який здійснюється шляхом використання вразливостей програмного забезпечення, підбору паролів або застосування соціальної інженерії. У результаті таких дій зловмисники отримують доступ до конфіденційної інформації, що може призвести до фінансових втрат, репутаційної шкоди та порушення прав суб’єктів персональних даних.

Значну небезпеку становлять шкідливі програмні засоби, зокрема віруси, трояни, шпигунські програми та програми-вимагачі. Вони здатні здійснювати прихований збір персональних даних, блокувати доступ до інформаційних ресурсів або знищувати дані. Поширення такого програмного забезпечення часто відбувається через електронну пошту, заражені вебресурси або незахищені зовнішні носії інформації.

Окрему групу загроз формують атаки, спрямовані на порушення доступності інформаційних ресурсів, зокрема атаки типу DDoS. Хоча їх основною метою є виведення систем з ладу, наслідком може стати також

втрата або компрометація персональних даних, що зберігаються в уражених системах.

Внутрішні загрози не менш небезпечні, ніж зовнішні. Вони пов’язані з діяльністю співробітників організацій, які мають законний доступ до персональних даних. Недостатній рівень підготовки персоналу, ігнорування правил інформаційної безпеки, використання слабких паролів або передавання облікових даних третім особам значно підвищують ймовірність витоку інформації. Крім того, навмисні дії з боку недобросовісних працівників можуть призвести до цілеспрямованого розголошення або модифікації персональних даних.

Суттєвий вплив на рівень загроз мають також хмарні сервіси та соціальні мережі. Використання сторонніх платформ для зберігання й обробки персональних даних часто супроводжується обмеженим контролем з боку користувачів і організацій. Неналежне налаштування параметрів безпеки або зміни в політиках конфіденційності провайдерів можуть стати причиною несанкціонованого доступу до інформації.

Таким чином, сучасні загрози для персональних даних є комплексними та потребують системного підходу до їх аналізу й нейтралізації. Це обумовлює необхідність розроблення ефективної методики захисту персональних даних, здатної адаптуватися до постійно змінюваного цифрового середовища..

Стрімкий розвиток інформаційно-комунікаційних технологій та активне впровадження цифрових сервісів у всі сфери суспільного життя зумовили суттєве зростання обсягів інформаційних ресурсів, що обробляються, передаються та зберігаються в електронному вигляді. Особливе місце серед таких ресурсів займають ПД, які мають високу цінність як для легітимних користувачів, так і для зловмисників. У зв’язку з цим проблема захисту інформаційних ресурсів від сучасних загроз набуває особливої актуальності.

Інформаційні ресурси у цифровому середовищі постійно піддаються впливу різноманітних загроз, які можуть призвести до порушення їх конфіденційності, цілісності та доступності. Сучасні загрози

характеризуються складністю, динамічністю та здатністю швидко адаптуватися до нових умов функціонування інформаційних систем. Для формування ефективної методики захисту персональних даних необхідно здійснити детальний аналіз основних видів таких загроз.

Інформаційна загроза — це потенційна або реальна можливість впливу на інформаційний ресурс, що може призвести до небажаних наслідків для суб'єктів інформаційних відносин. У цифровому середовищі загрози можуть бути як навмисними, так і ненавмисними, а також мати внутрішнє або зовнішнє походження (рис. 1.1).

Навмисні загрози, як правило, пов'язані з діяльністю кіберзлочинців, хакерських угруповань або недобросовісних співробітників, тоді як ненавмисні загрози виникають унаслідок технічних збоїв, людських помилок або недостатнього рівня організаційного забезпечення інформаційної безпеки.

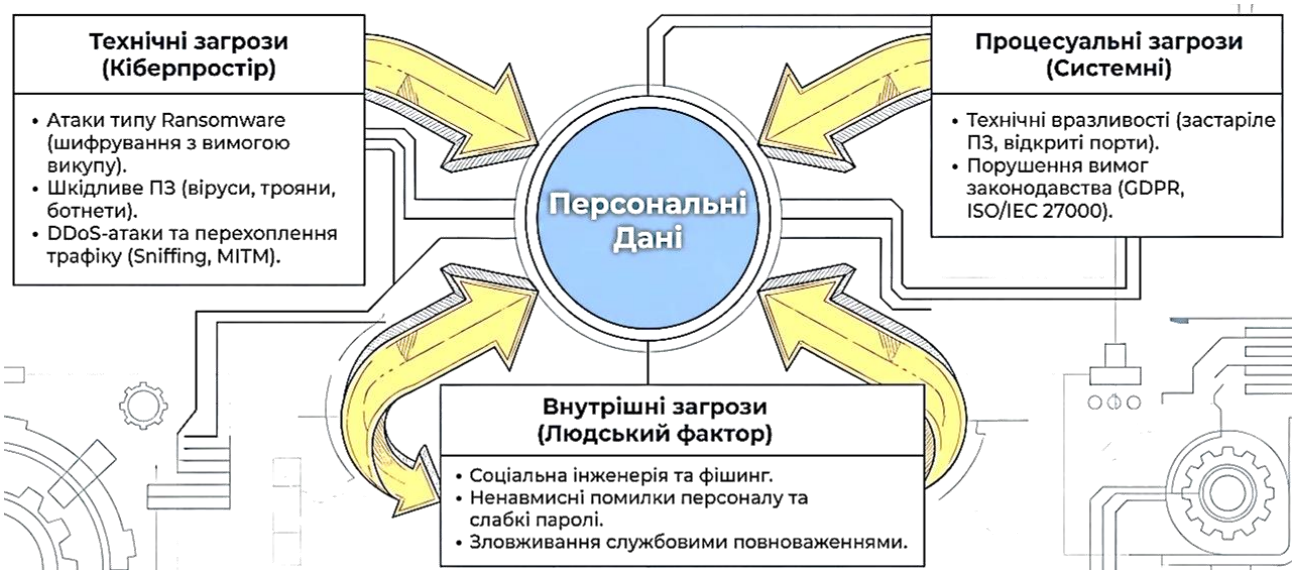

Рисунок 1.1. Узагальнена класифікація інформаційних загроз

Однією з найбільш небезпечних груп загроз для інформаційних ресурсів є кіберзагрози, що реалізуються шляхом атак на програмно-апаратні компоненти інформаційних систем. До таких загроз належать шкідливе програмне забезпечення, несанкціонований доступ, атаки на мережеву інфраструктуру та бази даних.

Особливу загрозу становлять:

- комп’ютерні віруси та троянські програми;
- шпигунське програмне забезпечення;
- бот-мережі;
- програми-вимагачі (ransomware).

Метою більшості кіберзагроз є викрадення ПД, порушення роботи інформаційних систем або отримання неправомірної фінансової вигоди. Атаки часто здійснюються з використанням автоматизованих засобів, що дозволяє зловмисникам одночасно впливати на значну кількість об’єктів.

Окрему увагу слід приділити атакам типу ransomware, які останніми роками стали однією з найсерйозніших загроз для інформаційних ресурсів. Суть таких атак полягає у шифруванні даних користувача або організації з подальшою вимогою викупу за їх відновлення.

Наслідками таких атак можуть бути:

- повна або часткова втрата ПД;
- зупинка діяльності організацій;
- значні фінансові збитки;
- порушення вимог законодавства щодо захисту ПД.

Особливо вразливими до таких загроз є державні установи, медичні та освітні заклади, де рівень технічного захисту часто є недостатнім.

Соціальна інженерія є одним із найпоширеніших методів отримання несанкціонованого доступу до інформаційних ресурсів. Вона базується на психологічному впливі на користувачів з метою спонукання їх до розкриття конфіденційної інформації.

Фішингові атаки можуть здійснюватися через:

- електронну пошту;
- месенджери;
- соціальні мережі;
- підроблені вебсайти.

Зловмисники маскують свої повідомлення під офіційні звернення банків, державних органів або відомих компаній. У результаті користувачі

самостійно передають свої логіни, паролі, платіжні дані та інші персональні відомості, що призводить до компрометації інформаційних ресурсів.

Внутрішні загрози виникають у межах організацій і пов’язані з діяльністю співробітників, які мають доступ до інформаційних ресурсів. Такі загрози можуть бути як умисними, так і ненавмисними.

Основними причинами внутрішніх загроз є:

- низький рівень обізнаності персоналу у сфері інформаційної безпеки;
- відсутність чітких регламентів доступу до даних;
- помилки під час обробки персональних даних;
- зловживання службовими повноваженнями.

Небезпека внутрішніх загроз полягає в тому, що вони часто залишаються непоміченими протягом тривалого часу, оскільки дії виконуються авторизованими користувачами.

Технічні уразливості є ще одним важливим джерелом загроз для інформаційних ресурсів. Вони виникають унаслідок помилок у програмному коді, неправильного налаштування систем або використання застарілого програмного забезпечення.

Зловмисники активно використовують такі уразливості для:

- несанкціонованого доступу до баз даних;
- підміни або знищення інформації;
- встановлення шкідливого програмного забезпечення.

Особливо актуальною є проблема безпеки вебзастосунків та хмарних сервісів, які часто обробляють значні обсяги ПД.

Зберігання та передача персональних даних без використання належних засобів захисту створюють значні ризики їх компрометації. Передавання інформації через незахищені канали зв’язку може призвести до її перехоплення, а зберігання на незахищених носіях — до витоку або втрати даних.

Недотримання принципів мінімізації даних, а також перевищення допустимих строків зберігання інформації підвищує ймовірність негативних наслідків у разі реалізації загроз.

Отже, сучасні загрози для інформаційних ресурсів у цифровому середовищі мають багатокомпонентний характер та поєднують технічні, організаційні й соціальні аспекти. Найбільш уразливими залишаються персональні дані, що обумовлює необхідність комплексного підходу до їх захисту.

Результати проведеного аналізу свідчать про те, що ефективна методика захисту персональних даних повинна враховувати різноманітність загроз, їх динамічний характер та роль людського фактора. Це створює теоретичну основу для подальшого дослідження методів і засобів захисту персональних даних, що буде розглянуто в наступних розділах дипломної роботи.

1.2 Аналіз засобів (методів) захисту персональних даних

У сучасному цифровому середовищі захист персональних даних реалізується за допомогою сукупності методів і засобів, які спрямовані на забезпечення конфіденційності, цілісності та доступності інформації. Ефективність системи захисту визначається не окремим інструментом, а комплексним поєднанням технічних, організаційних та правових заходів, що відповідають характеру оброблюваних даних і рівню загроз (рис. 1.2).

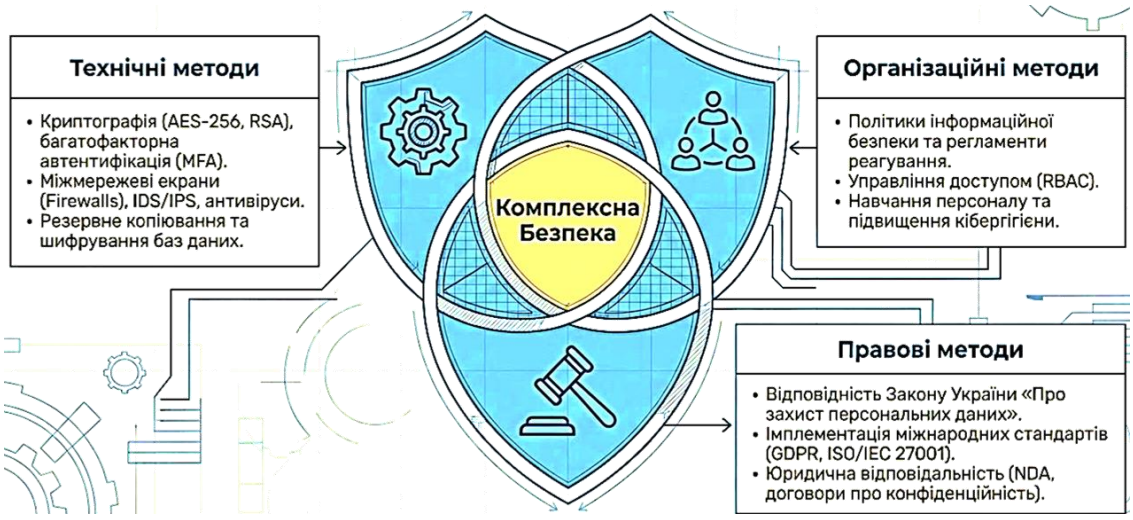

Рисунок 1.2. Засоби забезпечення кібербезпеки

Детально розглянемо кожен із них.

У сучасному цифровому середовищі технічні методи захисту персональних даних відіграють ключову роль у забезпеченні інформаційної безпеки. Вони спрямовані на запобігання несанкціонованому доступу, втраті, модифікації або знищенню персональних даних у процесі їх зберігання, обробки та передавання. Застосування технічних методів дозволяє реалізувати основні принципи захисту інформації — конфіденційність, цілісність і доступність.

Одним із найбільш ефективних технічних методів захисту персональних даних є криптографічний захист інформації. Він передбачає використання алгоритмів шифрування для забезпечення конфіденційності даних як під час зберігання, так і під час передавання мережею. Сучасні симетричні та асиметричні алгоритми шифрування дозволяють значно ускладнити несанкціонований доступ до інформації навіть у разі її перехоплення.

Крім шифрування, криптографічні методи включають використання електронного цифрового підпису та хеш-функцій. Ці засоби забезпечують автентичність даних, їх цілісність та неможливість відмови від авторства, що є особливо важливим у цифрових системах обробки персональних даних.

Важливим елементом технічного захисту персональних даних є системи ідентифікації та автентифікації користувачів. Вони дозволяють визначити, хто саме отримує доступ до інформаційних ресурсів, і підтвердити його особу. Найпоширенішими методами є використання паролів, смарт-карт, токенів, а також біометричних характеристик.

Після успішної автентифікації застосовуються механізми авторизації, які визначають рівень доступу користувача до персональних даних. Використання принципу мінімальних привілеїв дозволяє обмежити доступ лише до тієї інформації, яка необхідна для виконання службових обов’язків, що суттєво знижує ризик витоку даних.

Для захисту персональних даних у мережевому середовищі широко застосовуються міжмережеві екрани, системи виявлення та запобігання вторгненням, а також засоби сегментації мережі. Вони дозволяють контролювати мережевий трафік, блокувати підозрілі з’єднання та запобігати

несанкціонованим атакам ззовні.

Програмні засоби захисту включають антивірусне програмне забезпечення, системи контролю цілісності файлів та засоби захисту від шкідливого коду. Регулярне оновлення програмного забезпечення та встановлення патчів безпеки є обов’язковою умовою підтримання належного рівня захисту персональних даних.

Персональні дані часто зберігаються в базах даних або хмарних сервісах, що вимагає застосування спеціалізованих технічних методів захисту. До них належать шифрування баз даних, контроль доступу на рівні записів, аудит операцій із даними та використання механізмів резервного копіювання.

У хмарних середовищах особливу увагу приділяють захисту каналів передавання даних, ізоляції віртуальних ресурсів і контролю доступу до хмарної інфраструктури. Використання таких методів дозволяє мінімізувати ризики, пов’язані з розміщенням персональних даних на віддалених серверах.

Невід’ємною складовою технічних методів захисту персональних даних є резервне копіювання та відновлення інформації. Регулярне створення резервних копій дозволяє забезпечити доступність персональних даних у разі технічних збоїв, кібератак або фізичного пошкодження обладнання. Важливо, щоб резервні копії також були захищені від несанкціонованого доступу, зокрема шляхом шифрування.

Отже, технічні методи захисту персональних даних є необхідною складовою комплексної системи інформаційної безпеки. Їх ефективність значною мірою залежить від правильного поєднання з організаційними та правовими заходами, а також від постійного вдосконалення відповідно до розвитку цифрових технологій і загроз.

У системі захисту персональних даних організаційні методи займають особливе місце, оскільки вони визначають порядок, правила та відповідальність за обробку персональної інформації в організації. На відміну від технічних засобів, організаційні методи спрямовані на регламентацію діяльності персоналу та управління процесами обробки даних, що дозволяє мінімізувати ризики, пов’язані з людським фактором.

Одним із ключових організаційних методів є розроблення та впровадження політики захисту персональних даних. Така політика визначає основні принципи обробки персональної інформації, порядок доступу до неї, а також заходи щодо забезпечення конфіденційності та цілісності даних. Наявність чітко сформульованої політики дозволяє стандартизувати дії персоналу та забезпечити відповідність вимогам чинного законодавства.

Політика захисту персональних даних повинна охоплювати всі етапи життєвого циклу даних — від моменту їх збору до знищення або архівування. Вона також має регулярно переглядатися та оновлюватися з урахуванням змін у законодавстві та розвитку цифрових технологій.

Важливим організаційним методом захисту персональних даних є розмежування доступу до інформаційних ресурсів. Цей метод передбачає надання працівникам лише тих прав доступу, які необхідні для виконання їх службових обов’язків. Застосування принципу мінімальних привілеїв дозволяє суттєво знизити ризик несанкціонованого доступу або випадкового розголошення персональних даних.

Управління повноваженнями включає також процедури надання, зміни та скасування прав доступу, особливо у разі зміни посадових обов’язків або звільнення працівників. Чітка регламентація цих процесів є важливою умовою забезпечення інформаційної безпеки.

Організаційні методи захисту персональних даних передбачають призначення відповідальних осіб за організацію та контроль процесів обробки персональної інформації. У багатьох організаціях такі функції покладаються на уповноважену особу з питань захисту персональних даних або підрозділ інформаційної безпеки.

Чіткий розподіл відповідальності між керівництвом, адміністраторами систем і рядовими працівниками дозволяє уникнути дублювання функцій та підвищує ефективність контролю за дотриманням вимог безпеки. Визначення відповідальності також сприяє підвищенню дисципліни персоналу у сфері захисту персональних даних.

Одним із найважливіших організаційних методів захисту персональних

даних є навчання персоналу. Проведення регулярних тренінгів і інструктажів з питань інформаційної безпеки дозволяє підвищити рівень обізнаності працівників щодо актуальних загроз і правил безпечної роботи з персональними даними.

Навчання має охоплювати питання розпізнавання соціальної інженерії, безпечного використання електронної пошти, захисту облікових даних та відповідальності за порушення встановлених правил. Дослідження показують, що системне навчання персоналу значно знижує кількість інцидентів, пов’язаних із людським фактором.

Організаційні методи захисту персональних даних включають також управління ризиками інформаційної безпеки. Це передбачає регулярну ідентифікацію загроз, оцінювання їх ймовірності та потенційних наслідків, а також розроблення заходів щодо їх мінімізації.

Важливим елементом є контроль дотримання встановлених вимог і процедур. Для цього проводяться внутрішні перевірки, аудити та оцінювання ефективності заходів захисту. Отримані результати використовуються для вдосконалення системи захисту персональних даних та підвищення її надійності.

Отже, організаційні методи захисту персональних даних є необхідною складовою комплексної системи інформаційної безпеки. Їх поєднання з технічними та правовими заходами дозволяє створити ефективну та стійку систему захисту персональної інформації в цифровому середовищі.

Правові та нормативні методи захисту персональних даних є фундаментальною складовою системи інформаційної безпеки, оскільки вони визначають правові рамки обробки персональної інформації, встановлюють обов’язки суб’єктів інформаційних відносин та передбачають відповідальність за порушення вимог щодо захисту даних. Саме ці методи забезпечують реалізацію конституційного права людини на недоторканність приватного життя у цифровому середовищі.

Основою правового захисту персональних даних в Україні є Конституція України, яка гарантує право на невтручання в особисте і сімейне

життя та захист конфіденційної інформації про особу. На розвиток конституційних положень спрямований Закон України «Про захист персональних даних», який визначає правові засади обробки персональних даних, права суб'єктів даних та обов'язки володільців і розпорядників персональної інформації.

Закон встановлює принципи обробки персональних даних, зокрема законність, справедливість, пропорційність і цільове призначення. Дотримання цих принципів є обов'язковою умовою правомірної діяльності організацій у цифровому середовищі. Окрім того, законодавство передбачає необхідність отримання згоди суб'єкта персональних даних на їх обробку, за винятком випадків, визначених законом.

Важливим елементом правових методів захисту є закріплення прав суб'єктів персональних даних. До таких прав належать право на доступ до власних даних, право вимагати їх виправлення або видалення, а також право на захист від незаконної обробки чи поширення персональної інформації.

У цифровому середовищі реалізація цих прав потребує створення ефективних механізмів взаємодії між суб'єктами даних і володільцями інформації. Це включає розроблення прозорих політик конфіденційності, процедур розгляду звернень громадян та забезпечення своєчасного реагування на запити щодо персональних даних.

Окрім законів, важливу роль у захисті персональних даних відіграють підзаконні нормативні акти, державні стандарти та галузеві рекомендації. Вони конкретизують вимоги законодавства та визначають практичні аспекти його реалізації. Зокрема, до таких документів належать методичні рекомендації щодо обробки персональних даних та нормативи у сфері інформаційної безпеки.

На рівні організацій правові та нормативні методи реалізуються через розроблення внутрішніх документів, таких як положення про обробку персональних даних, політики конфіденційності, договори про нерозголошення інформації. Ці документи визначають порядок роботи з персональними даними, відповідальність працівників та санкції за

порушення встановлених правил.

Значний вплив на формування національної системи захисту персональних даних мають міжнародні правові акти. Одним із найбільш авторитетних документів у цій сфері є Загальний регламент захисту даних Європейського Союзу (GDPR), який встановлює високі стандарти захисту персональної інформації та принцип відповідальності організацій за її безпеку.

Міжнародні стандарти, зокрема серія ISO/IEC 27000, також відіграють важливу роль у нормативному забезпеченні захисту персональних даних. Їх застосування дозволяє гармонізувати підходи до інформаційної безпеки та підвищити рівень довіри до цифрових сервісів.

Правові методи захисту персональних даних передбачають встановлення юридичної відповідальності за порушення вимог законодавства. Вона може мати адміністративний, цивільно-правовий або кримінальний характер залежно від тяжкості правопорушення та наслідків для суб’єктів персональних даних.

Наявність чітко визначених санкцій сприяє підвищенню дисципліни у сфері обробки персональних даних та стимулює організації до впровадження ефективних заходів захисту. У цифровому середовищі це набуває особливого значення через масштабність і швидкість поширення інформації.

Таким чином, правові та нормативні методи захисту персональних даних забезпечують основу для формування комплексної системи інформаційної безпеки. Їх поєднання з технічними та організаційними заходами дозволяє ефективно захищати персональні дані та забезпечувати реалізацію прав суб’єктів інформації в цифровому середовищі.

1.3 Формалізована постановка завдання дослідження.

У сучасних умовах цифровізації суспільства проблема захисту персональних даних набуває особливої актуальності у зв’язку зі зростанням обсягів інформації, що обробляється в інформаційних системах, та ускладненням загроз інформаційній безпеці. Наявні підходи до захисту персональних даних часто мають фрагментарний характер і не забезпечують належного рівня безпеки в умовах динамічного цифрового середовища. Це зумовлює необхідність розроблення формалізованої методики захисту персональних даних, яка б враховувала комплекс сучасних загроз, нормативно-правові вимоги та технічні можливості інформаційних систем.

Об’єктом дослідження є процеси обробки та захисту персональних даних в інформаційних системах цифрового середовища.

Предметом дослідження є методи, засоби та моделі забезпечення захисту персональних даних, спрямовані на підвищення рівня їх конфіденційності, цілісності та доступності в умовах сучасних інформаційних загроз.

Метою дослідження є розроблення та обґрунтування методики захисту персональних даних у цифровому середовищі, яка забезпечує комплексний підхід до протидії загрозам інформаційної безпеки та відповідає вимогам чинного законодавства і міжнародних стандартів.

Для досягнення поставленої мети в роботі передбачається розв’язання таких основних завдань:

- проаналізувати сучасні загрози для інформаційних ресурсів систем та персональних даних;
- дослідити існуючі технічні, організаційні та правові методи захисту персональних даних;
- провести аналіз нормативно-правового забезпечення захисту персональних даних у цифровому середовищі;
- сформувати вимоги до методики захисту персональних даних з урахуванням особливостей цифрових інформаційних систем;

- розробити формалізовану модель процесу захисту персональних даних;
- обґрунтувати вибір засобів і методів захисту на основі оцінювання ризиків;
- оцінити ефективність запропонованої методики та визначити напрями її практичного застосування.

У межах формалізованої постановки завдання дослідження визначаються такі вхідні дані**:**

- характеристики інформаційної системи та її архітектури;
- перелік і категорії персональних даних, що обробляються;
- нормативно-правові вимоги щодо захисту персональних даних;
- перелік актуальних загроз та вразливостей;
- обмеження щодо ресурсів і функціональних можливостей системи.

Вихідними даними **є:**

- формалізована методика захисту персональних даних;
- модель процесу управління захистом персональних даних;
- рекомендації щодо впровадження технічних та організаційних заходів безпеки;
- критерії оцінювання ефективності системи захисту персональних даних.

Обмеження та припущення

У ході дослідження приймаються такі припущення:

- інформаційна система функціонує у відкритому цифровому середовищі;
- загрози інформаційній безпеці мають як зовнішній, так і внутрішній характер;
- захист персональних даних реалізується з урахуванням чинного законодавства України та міжнародних стандартів.

Обмеженнями дослідження є технічні можливості інформаційних систем, фінансові ресурси та рівень підготовки персоналу, що впливають на вибір конкретних методів і засобів захисту.

Таким чином, формалізована постановка завдання дослідження дозволяє чітко визначити цілі, завдання та межі роботи, а також створює основу для подальшого розроблення методики захисту персональних даних у цифровому середовищі.

Висновки до першого розділу

Підсумовуючи викладене в розділі можна зробити висновок. Аналіз сучасного стану інформаційної безпеки показав, що стрімкий розвиток цифрових технологій і масова цифровізація суспільних процесів створюють нові загрози для конфіденційності, цілісності та доступності персональної інформації. Сучасні кіберзагрози мають комплексний і динамічний характер: вони включають як зовнішні атаки (хакерські вторгнення, фішинг, шкідливе програмне забезпечення), так і внутрішні ризики, пов’язані з людським фактором або неправильним управлінням доступом до даних.

Було здійснено системний аналіз технічних методів захисту персональних даних. Зокрема, розглянуто криптографічні засоби, включаючи симетричне та асиметричне шифрування, хешування та електронний цифровий підпис, які забезпечують конфіденційність і цілісність інформації. Аналіз систем ідентифікації, автентифікації та авторизації показав, що багатофакторні механізми доступу та принцип мінімальних привілеїв значно знижують ризик несанкціонованого доступу. Окрему увагу приділено мережевим та програмним засобам захисту, таким як антивірусне ПЗ, міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), а також резервне копіювання та шифрування даних у базах даних і хмарних сервісах.

Організаційні методи захисту персональних даних виявились не менш важливими, ніж технічні. Розроблення внутрішніх політик і регламентів, чітке розмежування доступу та управління правами користувачів, призначення відповідальних осіб за захист даних та регулярне навчання персоналу забезпечують системність і дисципліну у сфері обробки

персональної інформації. Дослідження показало, що навчання персоналу та підвищення його обізнаності є ключовим фактором зниження ризиків, пов’язаних із людським фактором, який, за статистикою, є причиною більшості витоків даних.

Правові та нормативні методи захисту персональних даних визначають рамки, в яких повинна функціонувати система безпеки. Вивчення законодавства України, зокрема Закону України «Про захист персональних даних», положень Конституції України та міжнародних стандартів (GDPR, ISO/IEC 27000) дозволило окреслити обов’язки суб’єктів даних, права громадян на доступ та контроль за обробкою їх інформації, а також правові наслідки порушень. Цей аспект гарантує, що система захисту персональних даних не тільки технічно ефективна, а й законна, що особливо важливо для забезпечення довіри користувачів та партнерів.

У дипломній роботі була сформульована формалізована постановка завдання дослідження, що включає визначення об’єкта та предмета дослідження, мети та завдань, а також вхідних і вихідних даних, обмежень і припущень. Це створило методологічну основу для розробки комплексної методики захисту персональних даних, що дозволяє систематизувати підхід до захисту інформації та інтегрувати технічні, організаційні та правові засоби у єдину модель.

Отримані результати свідчать про необхідність комплексного підходу до захисту персональних даних у цифровому середовищі, де ефективність кожного методу залежить від взаємодії з іншими елементами системи. Впровадження запропонованої методики може підвищити рівень захисту персональних даних, знизити ризики витоків і несанкціонованого доступу, а також забезпечити відповідність законодавчим та міжнародним вимогам.

Таким чином, виконане дослідження підтверджує, що розробка системи захисту персональних даних має комплексний характер, який поєднує технічні, організаційні та правові заходи. Запропонована методика є практично застосовною і може бути використана як у державних, так і в

комерційних інформаційних системах для підвищення рівня інформаційної безпеки та створення безпечного цифрового середовища.

РОЗДІЛ 2. РОЗРОБЛЕННЯ МЕТОДИКИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИРОВОМУ СЕРЕДОВИЩІ

2.1 Оцінювання ризиків персональних даних у цифровому середовищі.

Оцінювання ризиків персональних даних є одним із ключових етапів розробки методики захисту інформації. Воно дозволяє визначити ймовірність виникнення загроз, оцінити їх потенційний вплив на об’єкти захисту та обґрунтувати необхідні заходи для мінімізації негативних наслідків. У цифровому середовищі ризики набувають особливої значущості через велику кількість загроз, високу швидкість обробки даних та складність сучасних інформаційних систем.

Ідентифікація загроз і вразливостей є першим та ключовим етапом оцінювання ризиків персональних даних у цифровому середовищі. Цей етап дозволяє визначити, які саме події або фактори можуть негативно впливати на інформаційні системи та персональні дані, а також які слабкі місця системи можуть бути використані для реалізації цих загроз.

Загрози для персональних даних можна класифікувати за кількома критеріями (рис. 1.3):

Технічні загрози:

Несанкціонований доступ до баз даних або мережевих ресурсів;

Атаки на мережеву інфраструктуру, включаючи DDoS-атаки та перехоплення трафіку;

Впровадження шкідливого програмного забезпечення (віруси, трояни, ransomware);

Втрати даних через збої апаратного чи програмного забезпечення;

Помилки налаштувань системи та програмних продуктів.

Людські та організаційні загрози:

Недотримання працівниками політик безпеки та правил обробки персональних даних;

Помилки при введенні або передачі даних;

Фішинг, соціальна інженерія та інші методи обману для отримання доступу до даних;

Зловмисні дії внутрішніх користувачів (наприклад, співробітників).

Правові та нормативні загрози:

Порушення вимог законодавства про захист персональних даних (наприклад, GDPR або Закон України «Про захист персональних даних»);

Недотримання внутрішніх регламентів, політик конфіденційності та договорів з контрагентами;

Використання зовнішніх сервісів та постачальників без належного контролю.

Вразливості інформаційної системи

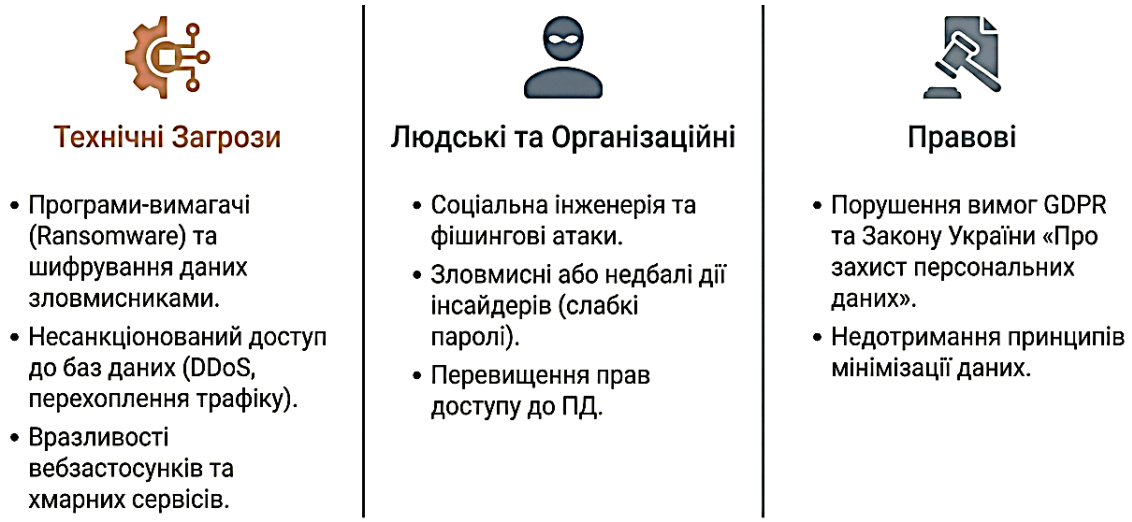

Рисунок 1.3. Класифікація загроз персональним даним

Вразливості – це слабкі місця системи, через які загрози можуть реалізуватись. Основні види вразливостей:

Технічні вразливості:

застаріле програмне забезпечення;

слабкі або стандартні паролі;

відсутність шифрування даних або багатофакторної автентифікації;

незахищена мережева інфраструктура (відкриті порти, відсутність брандмауерів).

Організаційні вразливості:

відсутність регламентів та політик роботи з персональними даними;

відсутність відповідальних осіб за інформаційну безпеку;

низький рівень підготовки персоналу щодо інформаційної безпеки.

Процесуальні та правові вразливості:

відсутність контролю за дотриманням законодавчих вимог;

недостатній аудит обробки персональних даних;

неповна або застаріла документація на внутрішні процеси.

Практичний підхід до ідентифікації

1. Аналіз архітектури системи – визначення критичних вузлів, де зберігаються або обробляються персональні дані.

2. Оцінка активів – перелік об’єктів, що потребують захисту (бази даних, сервери, хмарні сервіси, робочі станції).

3. Аналіз потенційних загроз – складання переліку технічних, людських та організаційних загроз.

4. Виявлення вразливостей – аудит безпеки, тестування на проникнення, оцінка відповідності системи стандартам безпеки.

5. Формування матриці загроз та вразливостей – для подальшої оцінки ймовірності їх реалізації та визначення рівня ризику.

Методи оцінки ризиків

Оцінка ризиків є ключовим етапом управління безпекою персональних даних у цифровому середовищі. Метою оцінки є визначення ймовірності реалізації загроз, оцінка їхнього потенційного впливу на інформаційні ресурси та обґрунтування заходів для мінімізації наслідків. У науковій та практичній літературі виділяють кілька основних методів оцінки ризиків: якісний, кількісний та змішаний.

Якісний метод

Якісна оцінка ризиків базується на експертному аналізі та визначенні ризику за категоріями, наприклад: низький, середній, високий.

Основні кроки:

1. Виявлення загроз і вразливостей .

2. Оцінка ймовірності реалізації кожної загрози за шкалою, наприклад:

Низька (малоймовірно)

Середня (можлива)

Висока (ймовірно)

3. Визначення рівня ризику як поєднання ймовірності та наслідків.

Переваги:

Простота застосування;

Не потребує складних математичних розрахунків;

Дозволяє швидко отримати уявлення про пріоритетні загрози.

Недоліки:

Суб’єктивність оцінок;

Важко порівнювати різні типи ризиків.

2. Кількісний метод

Кількісна оцінка ризиків дозволяє розрахувати числові значення ймовірності та наслідків, що забезпечує точну пріоритизацію ризиків.

Основна формула для розрахунку ризику:

R=P×LR = P \times LR=P×L

де:

RRR – рівень ризику;

PPP – ймовірність реалізації загрози (0–1);

LLL – величина потенційних втрат або шкоди (0–1).

Приклад розрахунку:

Загроза: несанкціонований доступ до бази даних;

Ймовірність реалізації: P=0,7P = 0,7P=0,7 (висока);

Потенційні наслідки: L=0,9L = 0,9L=0,9 (критичні);

Розрахунок: R=0,7×0,9=0,63R = 0,7 \times 0,9 = 0,63R=0,7×0,9=0,63.

На основі розрахованого значення ризику визначають пріоритет заходів (рис. 1.4):

R>0,6R > 0,6R>0,6 – високий пріоритет;

0,3<R≤0,60,3 < R \le 0,60,3<R≤0,6 – середній пріоритет;

R≤0,3R \le 0,3R≤0,3 – низький пріоритет.

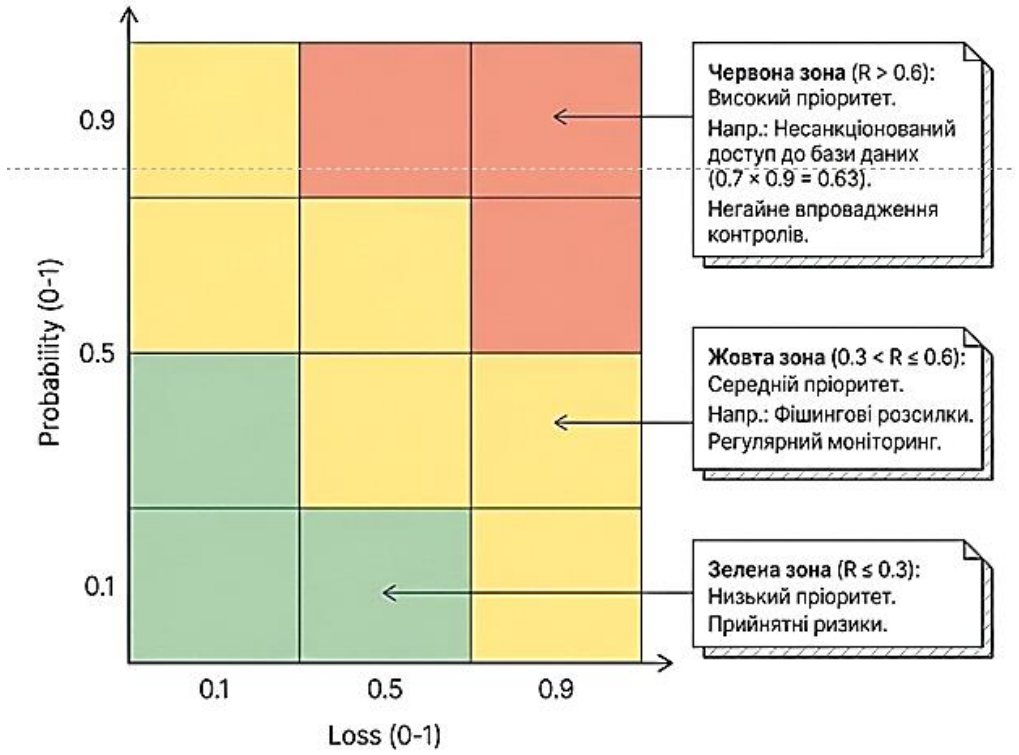

Рисунок 1.4. Пріоритетність кількісної оцінки ризиків

Переваги:

Можливість порівняння ризиків за числовими значеннями;

Чітка аргументація для керівництва при прийнятті рішень;

Застосовується для автоматизованих систем моніторингу.

Недоліки:

Потребує точних даних;

Вимагає кваліфікованих фахівців для проведення розрахунків.

3 . Змішаний метод

Змішаний (гібридний) метод поєднує переваги кількісного та якісного підходів.

Підхід:

Використовуються експертні оцінки для ймовірності реалізації загроз та потенційних наслідків;

Потім ці оцінки переводяться у числові значення і обчислюється рівень ризику за формулою R=P×LR = P \times LR=P×L;

Визначаються пріоритети та плануються заходи захисту.

Переваги:

Менше суб’єктивності, ніж у чисто якісних методах;

Легше застосовувати в організаціях, де частково є дані для кількісного аналізу;

Можливість інтеграції з матрицями ризиків та автоматизованими системами управління безпекою.

4. Інструменти для оцінки ризиків

На практиці для оцінки ризиків застосовують:

Матриці ризиків (визначення R = P × L для всіх загроз)

SWOT-аналіз для виявлення внутрішніх та зовнішніх ризиків;

FAIR (Factor Analysis of Information Risk) – метод кількісного аналізу інформаційних ризиків;

ISO/IEC 27005 – міжнародний стандарт управління ризиками інформаційної безпеки.

Пріоритизація ризиків

Після оцінки ризиків важливо визначити, які з них потребують першочергового реагування. Найвищий пріоритет мають ризики, які поєднують високу ймовірність реалізації та значні наслідки для організації чи суб’єктів персональних даних. На основі пріоритизації формується стратегія захисту персональних даних, яка визначає послідовність та інтенсивність заходів безпеки.

Документування та контроль ризиків

Результати оцінки ризиків повинні бути оформлені у вигляді таблиць або матриць ризиків, що дозволяє:

відстежувати зміни у рівні загроз;

планувати технічні та організаційні заходи захисту;

контролювати ефективність застосованих методів.

Таким чином, оцінювання ризиків персональних даних у цифровому

середовищі є ключовим етапом розробки методики захисту, оскільки дозволяє системно визначати пріоритети захисту, оптимізувати використання ресурсів та підвищувати ефективність заходів безпеки.

2.2 Визначення інструментарію захисту персональних даних на локальному рівні

Захист персональних даних на локальному рівні є ключовим елементом побудови ефективної системи інформаційної безпеки організації. Саме локальна інфраструктура (робочі станції, сервери, локальні мережі, внутрішні інформаційні системи) є основним середовищем накопичення, обробки та зберігання персональних даних працівників, клієнтів, контрагентів та інших суб’єктів даних. Відповідно, саме на цьому рівні виникає найбільша кількість ризиків, пов’язаних із несанкціонованим доступом, витоком або знищенням інформації.

Формування інструментарію захисту повинно здійснюватися з урахуванням вимог національного законодавства України та міжнародних нормативних актів, зокрема положень General Data Protection Regulation, що визначають принципи законності, прозорості, мінімізації даних, обмеження строків зберігання та забезпечення належного рівня безпеки обробки.

Інструментарій захисту на локальному рівні доцільно розглядати як багаторівневу систему, що включає:

нормативно-правові та організаційні заходи;

технічні (програмні та апаратні) засоби;

процедури моніторингу, контролю та реагування на інциденти;

механізми управління ризиками.

Методологічні засади формування інструментарію

Визначення інструментів захисту повинно базуватися на ризик-орієнтованому підході. На першому етапі проводиться ідентифікація активів (бази даних, сервери, інформаційні системи, архіви), після чого визначаються потенційні загрози та вразливості. Результатом є оцінка ризиків, що дозволяє

визначити пріоритетність впровадження захисних заходів.

До ключових принципів формування інструментарію належать:

1. Принцип мінімізації доступу — надання доступу лише тим працівникам, які безпосередньо здійснюють обробку персональних даних.
2. Принцип багаторівневого захисту (Defense in Depth) — використання кількох незалежних рівнів захисту.
3. Принцип безперервності захисту — постійний моніторинг і оновлення механізмів безпеки.
4. Принцип відповідності стандартам — орієнтація на міжнародні практики, зокрема вимоги ISO/IEC 27001.

Організаційний інструментарій

Організаційні заходи створюють нормативну основу для функціонування технічних засобів захисту.

1. Внутрішня нормативна база

Організація повинна розробити та затвердити:

Положення про обробку та захист персональних даних;

Політику інформаційної безпеки;

Інструкції щодо роботи з інформаційними системами;

Регламент реагування на інциденти.

Документація має визначати порядок збору, обробки, передачі та знищення персональних даних.

2. Управління доступом

Впроваджується чітка модель розмежування доступу (RBAC — role-based access control), що передбачає:

створення ролей відповідно до посадових обов’язків;

ведення журналів доступу;

регулярний перегляд прав користувачів;

автоматичне блокування облікових записів у разі звільнення працівника.

3. Управління персоналом

До інструментарію також належать:

підписання угод про нерозголошення (NDA);

перевірка рівня доступу під час кадрових змін;

проведення регулярних навчань з кібергігієни;

тестування знань працівників щодо правил безпеки.

Людський фактор є однією з найпоширеніших причин інцидентів, тому підвищення рівня обізнаності персоналу має стратегічне значення.

Технічний інструментарій

Технічні засоби забезпечують практичну реалізацію політики безпеки.

1. Засоби ідентифікації та автентифікації

багатофакторна автентифікація (MFA);

апаратні токени або смарт-карти;

біометрична автентифікація;

централізоване управління обліковими записами (Active Directory або аналогічні системи).

2. Криптографічний захист

Криптографія є одним із найефективніших способів захисту персональних даних. На локальному рівні застосовуються:

повнодискове шифрування робочих станцій;

шифрування баз даних;

використання захищених каналів зв’язку (VPN, TLS);

електронний підпис для підтвердження цілісності документів.

Шифрування дозволяє мінімізувати наслідки фізичного викрадення обладнання або несанкціонованого доступу до носіїв інформації.

3. Захист мережевої інфраструктури

використання міжмережевих екранів (firewall);

сегментація локальної мережі;

системи виявлення та запобігання вторгненням (IDS/IPS);

захист Wi-Fi мереж із застосуванням сучасних протоколів шифрування.

4. Захист кінцевих точок (Endpoint Security)

антивірусне програмне забезпечення;

EDR-системи (Endpoint Detection and Response);

контроль підключення зовнішніх носіїв (USB-контроль);

обмеження встановлення несанкціонованого ПЗ.

5. Резервне копіювання та відновлення

Ефективна система резервного копіювання передбачає:

автоматичне створення резервних копій;

зберігання копій у зашифрованому вигляді;

регулярну перевірку можливості відновлення;

використання принципу 3-2-1.

Системи моніторингу та контролю

Для забезпечення постійного контролю використовуються:

системи журналювання подій (логування);

SIEM-платформи для аналізу подій безпеки;

DLP-системи для запобігання витоку інформації;

аудит дій користувачів у критичних системах.

Моніторинг дозволяє оперативно виявляти підозрілу активність і мінімізувати наслідки інцидентів.

Фізичний захист інфраструктури

Окремим елементом інструментарію є фізична безпека:

обмежений доступ до серверних приміщень;

використання систем контролю доступу (СКУД);

відеоспостереження;

охоронна сигналізація;

контроль температурного режиму серверних приміщень.

Фізичний захист є невід’ємною складовою загальної системи безпеки, оскільки навіть найсучасніші програмні засоби не забезпечать захист у разі фізичного доступу до обладнання.

Оцінка ефективності та вдосконалення системи

Після впровадження інструментарію необхідно здійснювати:

регулярну оцінку ризиків;

внутрішні та зовнішні аудити;

тестування на проникнення (penetration testing);

аналіз інцидентів та розробку коригувальних заходів.

Система захисту персональних даних повинна постійно вдосконалюватися з урахуванням розвитку технологій та появи нових кіберзагроз.

2.3 Визначення інструментарію захисту персональних даних на мережному рівні

Захист персональних даних на мережному рівні є критично важливим елементом комплексної системи інформаційної безпеки організації. Якщо локальний рівень зосереджується на захисті окремих пристроїв і внутрішніх інформаційних систем, то мережний рівень охоплює передачу даних каналами зв'язку, взаємодію між сегментами мережі, віддалений доступ, а також підключення до глобальної мережі Інтернет.

Саме мережна інфраструктура є основним вектором зовнішніх кібератак, що можуть призвести до несанкціонованого доступу, перехоплення або модифікації персональних даних. Відповідно до принципів, закріплених у General Data Protection Regulation, контролер персональних даних зобов'язаний впроваджувати належні технічні та організаційні заходи для забезпечення безпеки передачі інформації, включаючи шифрування та забезпечення цілісності даних.

Формування інструментарію захисту на мережному рівні повинно ґрунтуватися на ризик-орієнтованому підході та враховувати специфіку інфраструктури (корпоративна мережа, філіальна структура, хмарні сервіси, віддалені робочі місця).

Аналіз загроз на мережному рівні

Основними загрозами для персональних даних у мережному середовищі є:

перехоплення даних під час передачі (sniffing);

атаки типу «людина посередині» (MITM);

несанкціоноване підключення до корпоративної мережі;

DDoS-атаки;

мережеве сканування та експлуатація вразливостей;

фішингові атаки через електронну пошту;

компрометація віддаленого доступу.

З урахуванням зазначених загроз формується багаторівнева система мережного захисту.

Міжмережевий екран (Firewall) як базовий інструмент

Міжмережевий екран є основним засобом фільтрації мережевого трафіку. Він контролює вхідні та вихідні з’єднання відповідно до встановлених правил безпеки.

Функції firewall:

блокування несанкціонованих підключень;

обмеження доступу до внутрішніх ресурсів;

фільтрація трафіку за IP-адресами, портами, протоколами;

ведення журналів подій.

Сучасні міжмережеві екрани нового покоління (NGFW) забезпечують глибоку перевірку пакетів (Deep Packet Inspection), що дозволяє виявляти шкідливу активність навіть у дозволеному трафіку.

Сегментація мережі

Сегментація мережі передбачає поділ корпоративної інфраструктури на ізольовані зони (VLAN, DMZ). Це дозволяє:

мінімізувати поширення атаки;

ізолювати сервери з персональними даними;

відокремити гостьову мережу від внутрішньої;

забезпечити контрольований доступ між сегментами.

Наприклад, база персональних даних повинна розміщуватися у внутрішньому сегменті з обмеженим доступом через окремий сервер прикладного рівня.

Криптографічний захист мережевих з’єднань

Передача персональних даних мережею повинна здійснюватися виключно із застосуванням сучасних криптографічних протоколів:

TLS для веб-з’єднань (HTTPS);

VPN для віддаленого доступу співробітників;

IPsec для захищених тунелів між філіями.

Шифрування забезпечує конфіденційність і цілісність даних навіть у разі перехоплення трафіку. Використання VPN є обов'язковим при роботі з персональними даними з віддалених робочих місць або публічних мереж Wi-Fi.

Системи виявлення та запобігання вторгненням (IDS/IPS)

IDS (Intrusion Detection System) здійснює моніторинг мережевого трафіку з метою виявлення підозрілої активності, тоді як IPS (Intrusion Prevention System) не лише виявляє, а й блокує загрози в реальному часі.

Застосування IDS/IPS дозволяє:

виявляти спроби злому;

блокувати атаки на сервери баз даних;

попереджати експлуатацію вразливостей.

Інтеграція таких систем із централізованими платформами управління безпекою підвищує оперативність реагування.

Захист електронної пошти та веб-трафіку

Оскільки електронна пошта є одним із головних каналів витоку інформації, необхідно впроваджувати:

антифішингові фільтри;

SPF, DKIM та DMARC для перевірки доменів;

антивірусну перевірку вкладень;

обмеження передачі конфіденційних даних через пошту.

Для веб-захисту застосовуються проксі-сервери та системи фільтрації контенту, які блокують доступ до шкідливих або небезпечних ресурсів.

Системи запобігання витоку даних (DLP)

На мережному рівні DLP-системи аналізують трафік і виявляють спроби передавання персональних даних за межі організації.

DLP дозволяє:

контролювати пересилання файлів;

відстежувати передачу конфіденційної інформації через месенджери;

блокувати несанкціоноване копіювання даних у хмарні сервіси.

Для комплексного контролю мережної інфраструктури доцільно використовувати системи управління подіями інформаційної безпеки (SIEM). Вони забезпечують:

збір логів з усіх мережевих пристроїв;

кореляцію подій;

автоматичне виявлення аномалій;

формування звітів для аудиту.

Такі системи сприяють своєчасному виявленню інцидентів та забезпечують доказову базу у разі порушення захисту персональних даних.

Забезпечення безперервності та відмовостійкості мережі

Захист персональних даних пов’язаний не лише з конфіденційністю, а й з доступністю інформації. Для цього впроваджуються:

резервні канали зв’язку;

балансування навантаження;

захист від DDoS-атак;

дублювання критичних мережевих пристроїв.

Наявність плану відновлення після інциденту (Disaster Recovery Plan) дозволяє мінімізувати простої та втрати даних.

Відповідність міжнародним стандартам

Формування мережного інструментарію захисту повинно відповідати міжнародним стандартам управління інформаційною безпекою, зокрема вимогам ISO/IEC 27001.

Зазначений стандарт передбачає впровадження контролів, що стосуються управління мережею, криптографії, контролю доступу та моніторингу подій безпеки.

2.4. Структурна схема методики захисту персональних даних та опис її складових

Розроблення методики захисту персональних даних у цифровому середовищі потребує системного підходу, що передбачає чітке визначення

взаємопов’язаних елементів, їх послідовності та логіки функціонування. Структурна схема методики є концептуальною моделлю, яка відображає етапи формування, впровадження, контролю та вдосконалення системи захисту персональних даних в організації.

Методика повинна відповідати вимогам національного законодавства та міжнародних нормативних документів, зокрема General Data Protection Regulation та стандарту ISO/IEC 27001, які визначають принципи безпеки обробки інформації, ризик-орієнтований підхід та необхідність постійного вдосконалення системи управління інформаційною безпекою.

Структурна схема методики захисту персональних даних може бути представлена як послідовність взаємопов’язаних блоків (рис. 1.5):

1. Ідентифікація та класифікація персональних даних
2. Аналіз загроз та оцінка ризиків
3. Формування політики та нормативної бази
4. Визначення та впровадження інструментарію захисту
   локальний рівень
   мережний рівень
5. Моніторинг та аудит
6. Реагування на інциденти
7. Оцінка ефективності та вдосконалення системи

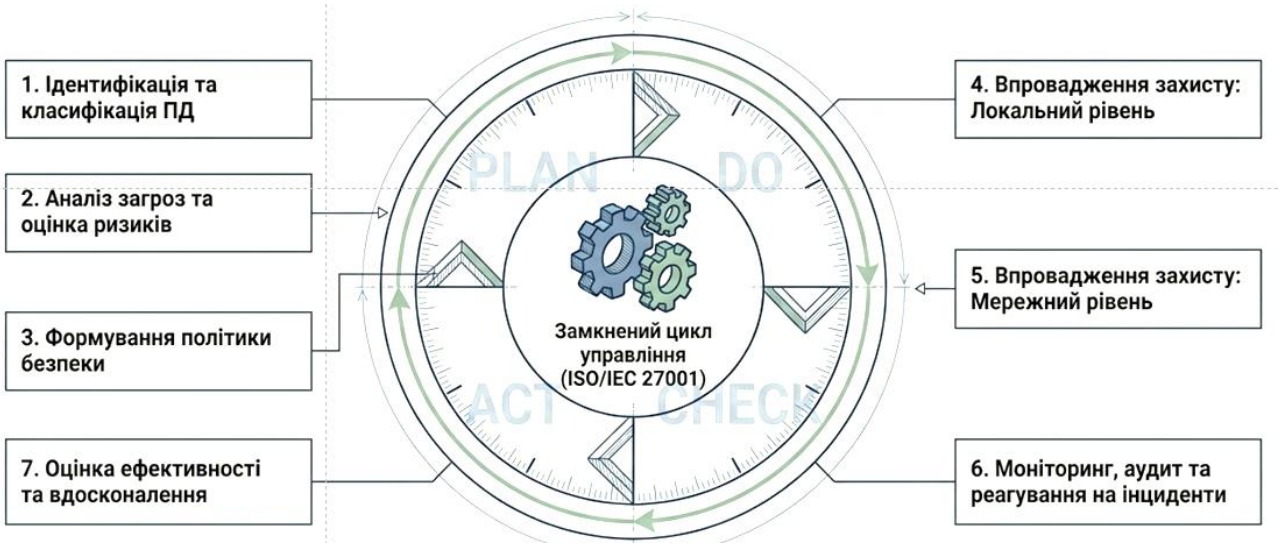

Рисунок 1.5. Структурна схема методики захисту персональних даних

Кожен із зазначених блоків виконує окрему функцію, але водночас інтегрований у єдину систему забезпечення безпеки.

Ідентифікація та класифікація персональних даних

Першим етапом є визначення:

які саме персональні дані обробляються;

з якою метою здійснюється їх обробка;

у яких інформаційних системах вони зберігаються;

хто має доступ до цих даних.

На цьому етапі формується реєстр баз персональних даних, а також визначається рівень їх чутливості (звичайні персональні дані, спеціальні категорії даних, біометричні тощо). Класифікація дозволяє встановити пріоритетність захисних заходів залежно від критичності інформації.

Аналіз загроз та оцінка ризиків

Другим етапом є проведення комплексної оцінки ризиків.

Процедура включає:

ідентифікацію потенційних загроз (зовнішніх і внутрішніх);

визначення вразливостей інформаційної системи;

оцінку ймовірності реалізації загрози;

визначення можливих наслідків.

Результатом є формування карти ризиків, яка дозволяє обґрунтовано визначити необхідний рівень захисту. Саме ризик-орієнтований підхід є основою сучасних стандартів інформаційної безпеки.

На основі оцінки ризиків розробляється внутрішня політика захисту персональних даних, яка визначає:

принципи обробки персональних даних;

порядок доступу до інформації;

процедури зберігання та знищення даних;

відповідальність посадових осіб;

порядок повідомлення про інциденти.

Політика є нормативною основою функціонування всієї системи захисту.

Центральним елементом структурної схеми є блок практичної реалізації заходів безпеки.

1. Локальний рівень

Передбачає:

розмежування доступу користувачів;

автентифікацію та авторизацію;

шифрування носіїв інформації;

антивірусний захист;

резервне копіювання.

2. Мережний рівень

Включає:

міжмережеві екрани;

сегментацію мережі;

VPN-з’єднання;

IDS/IPS-системи;

захист електронної пошти;

DLP-системи.

Комплексність впровадження технічних та організаційних засобів формує багаторівневий захист (Defense in Depth).

Після впровадження системи захисту необхідним є постійний контроль її функціонування.

Моніторинг включає:

аналіз журналів подій;

контроль доступу;

перевірку актуальності оновлень програмного забезпечення;

аудит відповідності політиці безпеки.

Аудит може бути внутрішнім або зовнішнім. Його результати дозволяють виявити недоліки та визначити напрями вдосконалення.

Методика повинна передбачати чіткий алгоритм дій у разі порушення безпеки персональних даних:

1. Виявлення інциденту.
2. Локалізація загрози.
3. Оцінка масштабу порушення.
4. Повідомлення відповідальних осіб та, за необхідності, регуляторних органів.
5. Відновлення нормального функціонування системи.
6. Аналіз причин інциденту та запровадження коригувальних заходів.

Оперативність реагування безпосередньо впливає на мінімізацію наслідків витоку або втрати даних.

Заключним етапом є оцінка ефективності методики.

Вона передбачає:

повторну оцінку ризиків;

аналіз інцидентів;

оновлення політик;

модернізацію технічних засобів;

підвищення кваліфікації персоналу.

Методика повинна функціонувати за принципом циклічності (PDCA — Plan–Do–Check–Act), що забезпечує її адаптацію до нових технологій та загроз.

Узагальнено структурну схему можна представити як замкнений цикл (рис. 1.6):

Такий підхід забезпечує:

системність управління захистом персональних даних;

відповідність законодавчим вимогам;

зниження рівня інформаційних ризиків;

підвищення рівня довіри до організації.

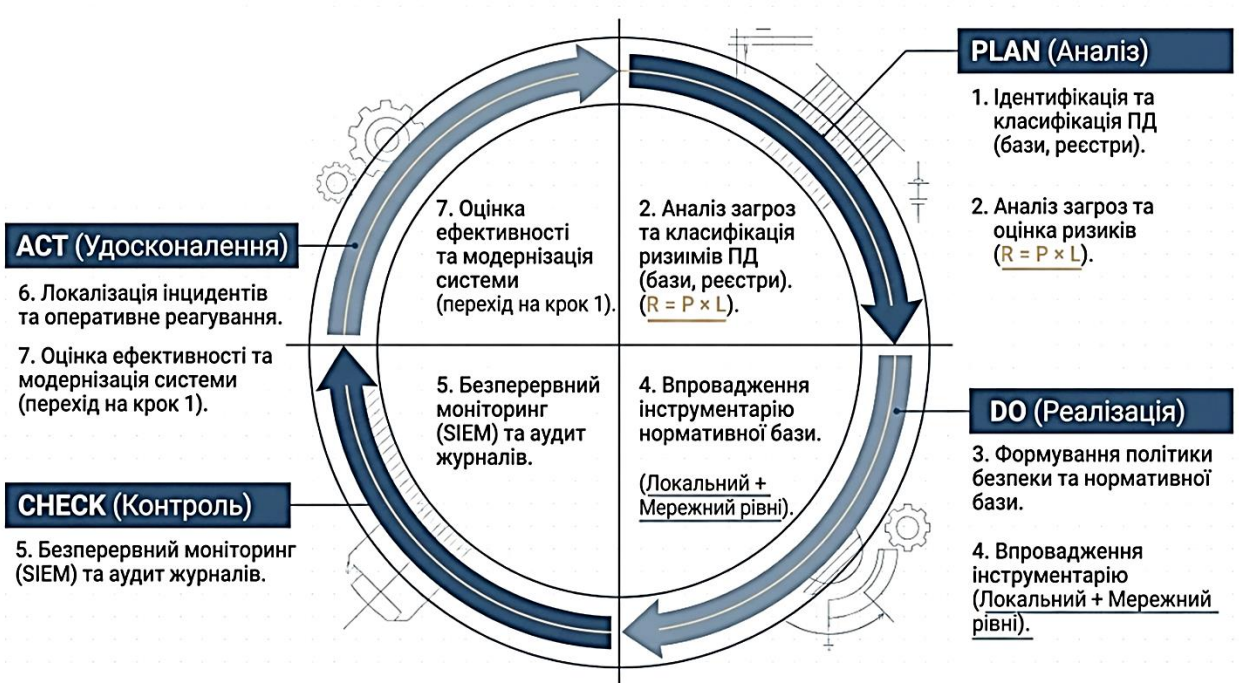

Рисунок 1.6. Узагальнено структурну схему реагування на кіберзагрози

Висновки до другого розділу

У другому розділі дипломної роботи було детально розглянуто основні підходи та інструменти, які використовуються для захисту персональних даних у цифровому середовищі, зокрема на локальному та мережному рівнях, а також створена структурна схема методики захисту персональних даних, що відображає взаємодію основних компонентів системи захисту інформації. Проведений аналіз дозволяє зробити кілька важливих висновків щодо необхідності та ефективності застосування різноманітних заходів безпеки для забезпечення конфіденційності, цілісності та доступності персональних даних у цифровому середовищі.

Захист персональних даних на локальному рівні є основою для забезпечення базової безпеки на рівні окремих пристроїв і інформаційних систем. Це включає захист даних, що зберігаються на комп’ютерах, серверах та інших фізичних носіях, а також контроль доступу до цих даних. Важливими елементами є використання антивірусних програм, засобів шифрування, систем резервного копіювання, а також політик безпеки для користувачів, що визначають, хто і на яких умовах має доступ до персональних даних. Це дозволяє знизити ризики, пов'язані з несанкціонованим доступом до даних, їх пошкодженням або втратою.

Інструментарій захисту персональних даних на мережному рівні дозволяє захистити інформацію під час її передачі через мережу, що є критично важливим у сучасному цифровому середовищі, де велика частина даних передається по Інтернету або через корпоративні мережі. Засоби захисту мережі включають міжмережеві екрани, криптографічні протоколи (TLS, VPN), системи виявлення та запобігання вторгненням (IDS/IPS), а також системи контролю за витоком інформації (DLP). Ці заходи дозволяють запобігти перехопленню, маніпуляціям або викраденню даних під час їх передачі між різними користувачами чи системами. Наприклад, застосування VPN-з'єднань для віддалених співробітників або шифрування веб-трафіку гарантує, що передача персональних даних відбувається з максимальним рівнем захисту.

Структурна схема методики захисту персональних даних**,** представлена в розділі, є ефективним інструментом для впровадження комплексної системи захисту персональних даних у межах організації. Вона містить чітко визначені етапи, такі як ідентифікація та класифікація даних, аналіз ризиків, розробка політики безпеки, впровадження технічних та організаційних заходів, моніторинг і аудит, а також реакція на інциденти та вдосконалення системи. Кожен з цих етапів має на меті забезпечення того, щоб персональні дані були захищені на всіх етапах їх життєвого циклу: від збору та обробки до зберігання та знищення.

Оцінка ризиків і загроз є основою для побудови ефективної методики захисту. Визначення ймовірності виникнення різних загроз, а також оцінка їх можливих наслідків, дозволяє правильно налаштувати заходи безпеки. За допомогою ризик-орієнтованого підходу організація може обрати найбільш критичні для неї заходи та направити ресурси на їх впровадження, мінімізуючи можливі втрати або шкоду.

Політика безпеки та нормативно-правова база є важливою складовою методики. Вона визначає не лише правила та процедури, яких мають дотримуватись співробітники, а й забезпечує юридичну основу для виконання вимог законодавства, зокрема в рамках Загального регламенту захисту даних Європейського Союзу (GDPR) та національних нормативних актів, таких як Закон України «Про захист персональних даних». Важливим є формулювання чітких стандартів доступу до даних, їх обробки, зберігання та передачі, а також процедур повідомлення про порушення безпеки.

Моніторинг, аудит та реагування на інциденти — це механізми, що забезпечують постійну перевірку ефективності впроваджених заходів і дозволяють оперативно виявляти порушення або спроби несанкціонованого доступу. Моніторинг включає збір і аналіз журналів подій, перевірку безпеки систем і мереж, а також оцінку актуальності використаних інструментів безпеки. Аудит забезпечує зовнішню або внутрішню перевірку відповідності політиці безпеки та стандартам. Реагування на інциденти забезпечує швидку локалізацію і ліквідацію наслідків атак або витоків даних.

Циклічність та вдосконалення методики захисту персональних даних гарантує її адаптацію до нових загроз і технологій. Оцінка ефективності, тестування систем на проникнення та регулярне оновлення заходів безпеки дозволяють організаціям підтримувати високий рівень захисту і швидко реагувати на нові виклики.

Загалом, розроблена методика захисту персональних даних є багаторівневою, комплексною системою, яка охоплює всі аспекти безпеки — від організаційних заходів до впровадження технічних засобів і контролю за їх виконанням. Вона дозволяє організаціям не лише виконувати вимоги законодавства щодо захисту персональних даних, а й забезпечувати належний рівень кібербезпеки в умовах цифрових трансформацій.

Впровадження таких систем забезпечує високий рівень захисту інформації, підвищує довіру з боку клієнтів і партнерів, а також мінімізує ймовірність виникнення серйозних наслідків у разі інцидентів з безпекою даних. Враховуючи постійно змінювані умови на ринку кібербезпеки, організаціям важливо постійно вдосконалювати свою методику захисту персональних даних, щоб відповідати сучасним вимогам і технологіям.

РОЗДІЛ 3 АПРОБАЦІЯ МЕТОДИКИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВОМУ СЕРЕДОВИЩІ.

3.1. Аналіз вхідних даних та інформаційного (цифрового) середовища

Апробація розробленої методики захисту персональних даних у цифровому середовищі передбачає її практичне застосування в умовах конкретної організації або змодельованої інформаційної системи. Першим і ключовим етапом такого процесу є комплексний аналіз вхідних даних та особливостей інформаційного (цифрового) середовища, в якому здійснюється обробка персональних даних.

Структурна схема проведення апробації подана на рис. 1.7.

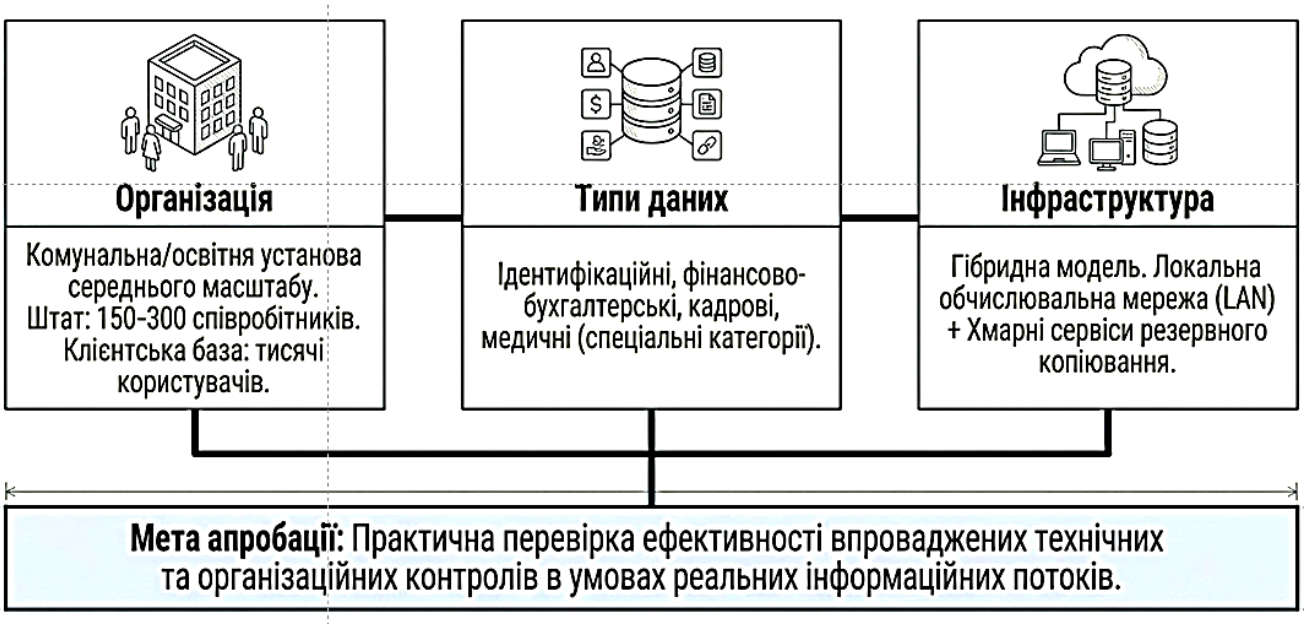

Рисунок 1.7. Схема проведення апробації

Метою цього етапу є визначення складу персональних даних, характеристик інформаційної інфраструктури, наявних засобів захисту, потенційних загроз і вразливостей. Такий підхід відповідає ризик-орієнтованій моделі управління інформаційною безпекою, що закріплена в ISO/IEC 27001, а також принципам безпеки обробки даних, визначеним у General Data Protection Regulation.

Апробація розробленої методики захисту персональних даних здійснюється на базі умовної організації середнього масштабу, діяльність якої пов’язана з регулярною обробкою значних обсягів персональних даних. Для цілей дослідження об’єктом апробації визначено комунальну установу (наприклад, заклад вищої освіти або адміністративну установу), що має розгалужену інформаційну інфраструктуру та багаторівневу систему доступу до даних.

Загальна характеристика організації подана на рис. 1.8.

Рисунок 1.8. Характеристика організації

Організація функціонує як багатопрофільна структура з кількістю працівників близько 150–300 осіб та контингентом користувачів (клієнтів/здобувачів послуг) до кількох тисяч осіб. Основні напрями діяльності пов’язані з:

веденням кадрового обліку;

наданням адміністративних або освітніх послуг;

фінансово-бухгалтерською діяльністю;

електронним документообігом;

взаємодією з державними реєстрами та іншими інформаційними системами.

У процесі діяльності організація виступає володільцем і розпорядником персональних даних відповідно до вимог чинного законодавства України та

принципів, закріплених у General Data Protection Regulation (у частині імплементації європейських підходів до захисту даних).

В організації функціонують такі структурні підрозділи:

Адміністраці, відділ кадрів, бухгалтерія, IT-відділ

профільні підрозділи (кафедри, відділи, служби тощо).

Обробка персональних даних здійснюється децентралізовано, однак з централізованим адмініструванням облікових записів через IT-відділ. Відповідальна особа за захист персональних даних призначена наказом керівника установи.

Характеристика інформаційної (цифрової) інфраструктури наведено на рис. 1.9.

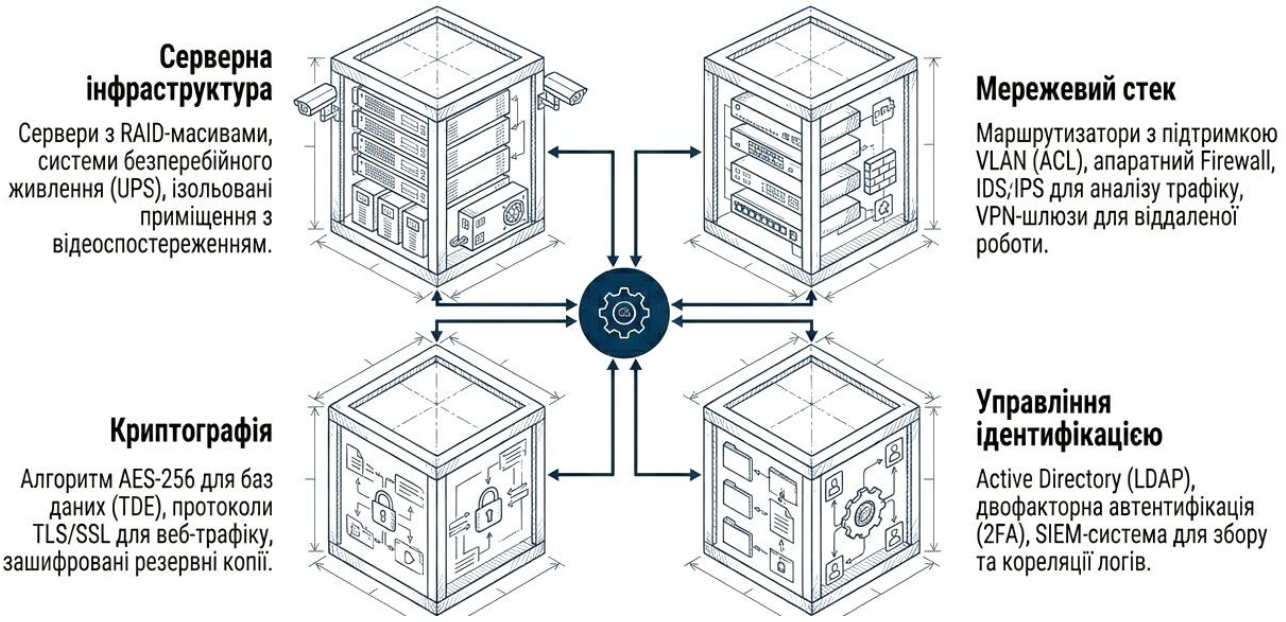

Рисунок 1.9. Характеристика інформаційної (цифрової) інфраструктури

Цифрове середовище організації включає:

локальну обчислювальну мережу (LAN);

серверну інфраструктуру (файловий сервер, сервер баз даних, поштовий сервер);

робочі станції користувачів (Windows/Linux);

мережеве обладнання (маршрутизатори, комутатори);

корпоративну електронну пошту;

систему електронного документообігу;

бухгалтерське програмне забезпечення;

веб-сайт із формами зворотного зв’язку;

використання хмарних сервісів для зберігання та резервного копіювання даних.

Серверне обладнання розміщене в окремому приміщенні, що має обмежений фізичний доступ. Частина сервісів може бути винесена в хмарне середовище (гібридна модель інфраструктури).

Характеристика інформаційних ресурсів

До основних інформаційних активів організації належать:

база персональних даних працівників;

база персональних даних клієнтів/здобувачів послуг;

фінансові та бухгалтерські дані;

електронні архіви документів;

внутрішня службова кореспонденція.

Оброблювані персональні дані включають:

ідентифікаційні відомості;

контактну інформацію;

фінансові реквізити;

дані про трудову діяльність;

у визначених випадках — спеціальні категорії персональних даних.

Обсяг інформації оцінюється як середній або високий, що зумовлює підвищені вимоги до рівня її захисту.

Поточний стан системи захисту

На момент апробації в організації впроваджені такі заходи:

базове розмежування доступу до інформаційних ресурсів;

використання антивірусного програмного забезпечення;

наявність міжмережевого екрана;

періодичне резервне копіювання;

ведення журналів подій.

Водночас виявлено низку недоліків:

відсутність повної сегментації мережі;

недостатня формалізація політики захисту персональних даних;

відсутність централізованої системи моніторингу інцидентів;

обмежене використання багатофакторної автентифікації.

Ці фактори створюють підґрунтя для практичного впровадження та перевірки ефективності розробленої методики.

Обраний об’єкт апробації характеризується:

наявністю різнорівневих інформаційних потоків;

значним обсягом персональних даних;

поєднанням локальної та мережної інфраструктури;

типовими для більшості організацій кіберризиками.

Це дозволяє вважати його репрезентативною моделлю для перевірки ефективності запропонованої методики захисту персональних даних у цифровому середовищі.

Аналіз складу вхідних персональних даних є одним із ключових етапів апробації методики захисту, оскільки саме від характеру, обсягу та чутливості оброблюваної інформації залежить вибір відповідних організаційних і технічних заходів безпеки. Даний етап передбачає ідентифікацію категорій персональних даних, джерел їх надходження, цілей обробки, строків зберігання та рівня критичності.

Відповідно до принципів обробки персональних даних, визначених у General Data Protection Regulation, персональні дані повинні бути адекватними, релевантними та обмеженими необхідним обсягом відповідно до мети їх обробки (принцип мінімізації даних). Тому під час аналізу важливо встановити, чи не відбувається надлишковий збір інформації.

У межах досліджуваного об’єкта апробації вхідні персональні дані можна умовно поділити на такі групи:

До цієї категорії належать відомості, що дозволяють однозначно ідентифікувати фізичну особу:

прізвище, ім’я, по батькові;

дата та місце народження;

серія та номер паспорта;

реєстраційний номер облікової картки платника податків;

унікальні внутрішні ідентифікатори (табельний номер, номер особової справи).

Ці дані є базовими для формування особових справ і ведення обліку.

Контактна інформація забезпечує комунікацію з суб’єктом персональних даних:

адреса проживання;

номер телефону;

електронна пошта;

поштова адреса для листування.

Контактні дані часто використовуються в електронних інформаційних системах, що підвищує ризик їх несанкціонованого розповсюдження.

У досліджуваному цифровому середовищі обробляються також:

відомості про освіту;

дані про трудовий стаж;

інформація про посаду;

розмір заробітної плати;

банківські реквізити;

дані про податкові відрахування.

Такі дані мають підвищений рівень конфіденційності через їх фінансовий характер.

У визначених випадках можуть оброблятися спеціальні категорії даних, зокрема:

медична інформація;

відомості про стан здоров’я;

дані про інвалідність;

біометричні дані (за наявності систем доступу);

інформація, що стосується соціального статусу.

Обробка таких даних потребує підвищеного рівня захисту, додаткового правового обґрунтування та суворого контролю доступу.

Вхідні персональні дані надходять до інформаційної системи через різні канали:

паперові заяви та анкети з подальшим внесенням до електронної бази;

електронні форми на веб-сайті;

електронну пошту;

інтеграцію з іншими інформаційними системами;

обмін даними з державними реєстрами.

Кожен із зазначених каналів створює окремі ризики:

можливість перехоплення даних у разі незахищеного з’єднання;

помилки оператора при ручному введенні інформації;

фішингові атаки через електронну пошту;

несанкціонована інтеграція з зовнішніми системами.

Під час апробації було встановлено, що:

загальна кількість суб’єктів персональних даних становить кілька тисяч осіб;

інформація зберігається у структурованих електронних базах даних;

частина даних дублюється у паперовому архіві;

частина обробляється у хмарному середовищі.

Наявність дублювання підвищує ризик витоку інформації та потребує чіткої регламентації строків зберігання та порядку знищення даних.

Для подальшого застосування методики захисту здійснено оцінку критичності даних за такими критеріями:

можливі фінансові втрати у разі витоку;

репутаційні ризики для організації;

правові наслідки;

шкода для суб’єкта персональних даних.

За результатами аналізу встановлено, що найбільш критичними є:

фінансові реквізити;

ідентифікаційні номери;

медичні відомості;

службові та кадрові документи.

Ці категорії потребують підвищених заходів захисту, включаючи шифрування, обмеження доступу та журналювання операцій.

Під час аналізу перевірено, чи відповідає обсяг зібраних персональних даних заявленим цілям обробки. Виявлено окремі випадки надлишкового збору інформації, що не є критично необхідною для виконання функцій організації.

У межах апробації методики рекомендовано:

переглянути перелік обов’язкових полів у формах збору даних;

скоротити строки зберігання частини інформації;

впровадити регулярний аудит актуальності персональних даних.

Проведений аналіз складу вхідних персональних даних дозволив:

систематизувати категорії оброблюваної інформації;

визначити найбільш чутливі групи даних;

встановити основні джерела надходження;

виявити потенційні вразливості;

сформувати основу для подальшої оцінки ризиків.

Аналіз джерел надходження та каналів обробки персональних даних є важливим етапом апробації методики захисту, оскільки дозволяє визначити точки входу інформації в систему, маршрути її руху та потенційні зони ризику. Саме на цих етапах найчастіше виникають загрози несанкціонованого доступу, витоку або спотворення даних.

Відповідно до принципів безпечної обробки інформації, закріплених у General Data Protection Regulation, організація повинна забезпечити належний рівень технічного та організаційного захисту персональних даних на всіх етапах їх життєвого циклу — від моменту отримання до знищення або архівування.

У межах об’єкта апробації встановлено такі джерела надходження персональних даних:

Найпоширенішим джерелом є добровільне надання інформації фізичною особою під час:

подання заяви про прийняття на роботу;

укладення договору;

реєстрації в електронній системі;

заповнення анкети або форми зворотного зв’язку.

Ризики:

надмірний збір інформації;

помилки при введенні даних;

відсутність шифрування під час онлайн-заповнення форм.

Дані можуть надходити у паперовому вигляді та згодом вноситися до електронної системи.

Ризики:

несанкціонований доступ до паперових архівів; помилки при ручному введенні; зберігання копій без належного контролю.

Персональні дані можуть надходити через: електронну пошту; месенджери; захищені веб-форми; корпоративні портали.

Ризики:

фішингові атаки;

заражені вкладення;

передача інформації через незахищені канали зв’язку.

Організація може отримувати персональні дані через автоматизований обмін із:

державними реєстрами;

банківськими установами;

підрядними організаціями;

хмарними сервісами.

Ризики:

неконтрольований доступ через API;

компрометація зовнішнього сервісу;

помилки синхронізації даних.

Після надходження інформація проходить декілька етапів обробки в межах цифрового середовища.

Критично важливим є обмеження доступу до цієї функції лише уповноваженим працівникам.

Персональні дані зберігаються:

у централізованих базах даних;

у файлових архівах;

у хмарних сховищах;

на резервних носіях.

Основні ризики:

несанкціонований доступ;

відсутність шифрування;

недостатній контроль резервних копій.

У процесі діяльності організації дані можуть передаватися між структурними підрозділами через:

локальну мережу;

електронну пошту;

внутрішні інформаційні системи.

Для наочності під час апробації було сформовано карту інформаційних потоків, яка відображає:

1. Точки входу даних (веб-форми, паперові документи, інтеграції).
2. Центральне сховище (сервер баз даних).
3. Канали внутрішньої передачі.
4. Канали зовнішньої передачі.
5. Архівування та резервне копіювання.

Такий підхід дозволяє визначити «вузькі місця» системи — ділянки, де існує підвищений ризик компрометації.

У ході аналізу встановлено такі потенційні проблеми:

відсутність обов’язкового використання HTTPS на всіх веб-формах;

передача файлів із персональними даними через електронну пошту без шифрування;

зберігання частини архівів без обмеження фізичного доступу;

відсутність централізованого контролю інтеграцій із зовнішніми сервісами.

Ці фактори створюють ризик витоку або несанкціонованої зміни інформації.

За результатами аналізу рекомендовано:

впровадити обов’язкове використання захищених протоколів передачі даних (HTTPS, VPN);

застосовувати шифрування вкладень у службовій електронній пошті;

централізувати управління інтеграціями з зовнішніми системами;

обмежити використання месенджерів для передачі конфіденційної інформації;

Для ефективної апробації методики необхідно дослідити:

архітектуру мережі (наявність сегментації, DMZ);

тип серверного обладнання;

операційні системи та їх актуальність;

наявність міжмережевих екранів;

використання VPN-з’єднань;

системи резервного копіювання;

системи журналювання подій.

Також аналізується рівень централізації управління обліковими записами та наявність політик доступу.

Фактичний стан захисту порівнюється з вимогами нормативних документів та запропонованою методикою.

На основі аналізу інфраструктури визначаються типові загрози:

несанкціонований доступ до баз даних;

компрометація облікових записів;

витік інформації через електронну пошту;

шкідливе програмне забезпечення;

фізичний доступ до серверного обладнання;

людський фактор.

Виявлені вразливості дозволяють оцінити ризики та визначити, які елементи методики потребують першочергового впровадження або доопрацювання.

Результатом аналізу вхідних даних та цифрового середовища є:

перелік активів, що підлягають захисту;

класифікація персональних даних;

визначення рівня ризику;

оцінка відповідності чинному законодавству;

визначення пріоритетних напрямів удосконалення.

Ці параметри є базою для подальшого впровадження та тестування розробленої методики захисту персональних даних.

3.2 Перелік апаратних та програмних засобів захисту цифрових даних.

Для забезпечення ефективної апробації розробленої методики захисту персональних даних необхідно детально описати всі наявні та рекомендовані засоби захисту, що використовуються на різних рівнях цифрового середовища. Комплексне поєднання апаратних та програмних рішень забезпечує багаторівневий захист даних, зменшуючи ймовірність несанкціонованого доступу, витоку чи пошкодження інформації.

1. Апаратні засоби захисту

Апаратні засоби забезпечують фізичну безпеку, надійність зберігання даних та контроль доступу до цифрових ресурсів.

Серверне обладнання та системи зберігання даних

Сервери баз даних та файлові сервери – центральний вузол зберігання персональних даних, забезпечують контроль доступу та підтримку політик безпеки.

RAID-масиви та NAS/SAN-системи – підвищують надійність зберігання, забезпечують автоматичне дублювання даних та резервування.

Системи безперебійного живлення (UPS) – гарантують стабільну роботу серверного обладнання при перебоях електропостачання.

Стабілізатори напруги та кондиціонування серверних приміщень – зменшують ризик пошкодження апаратури через нестабільну електромережу або перегрів.

Маршрутизатори та комутатори з підтримкою VLAN та Access Control Lists (ACL) – дозволяють сегментувати мережу та контролювати маршрутизацію даних.

Міжмережеві екрани (Firewall) – забезпечують контроль і фільтрацію трафіку між внутрішньою мережею та Інтернетом.

VPN-шлюзи та апаратні VPN-концентратори – організовують захищені канали віддаленого доступу для співробітників.

Апаратні засоби захисту від DDoS-атак – дозволяють виявляти та блокувати масові атаки на мережеву інфраструктуру.

Системи електронного контролю доступу (електронні картки, біометричні сканери) – обмежують фізичний доступ до серверних приміщень та критичних робочих місць.

Відеоспостереження та сигналізація – моніторинг і фіксація всіх спроб доступу.

Фізичні замки та сейфи для носіїв інформації – зберігання резервних копій та документації.

2. Програмні засоби захисту

Програмні засоби відповідають за захист інформації на логічному рівні та контроль доступу користувачів.

Засоби шифрування

Шифрування баз даних (TDE – Transparent Data Encryption, AES-256) – забезпечує захист даних у стані спокою.

Шифрування локальних і портативних носіїв (BitLocker, VeraCrypt) – захист даних на робочих станціях та зовнішніх носіях.

Шифрування електронної пошти (S/MIME, PGP) – захист від перехоплення конфіденційної інформації.

TLS/SSL та VPN – шифрування даних при передачі через мережу.

Антивірусні та антишкідливі програми

Антивірусні пакети для серверів та робочих станцій (ESET, Kaspersky, Symantec) – виявлення та блокування шкідливого ПЗ.

Антишпигунські програми та персональні файрволи – контроль локального доступу та поведінки додатків.

Системи виявлення та запобігання вторгненням (IDS/IPS) – аналіз трафіку та блокування підозрілих активностей.

Системи контролю доступу та управління обліковими записами

Active Directory / LDAP – централізоване управління користувачами та правами доступу.

Системи управління доступом на основі ролей (RBAC) – обмеження доступу залежно від посади та функцій користувача.

Двохфакторна автентифікація (2FA) – підвищує рівень безпеки при вході до систем.

Засоби резервного копіювання та відновлення

Локальні та хмарні резервні копії (Veeam, Acronis, Microsoft Azure Backup) – гарантія збереження даних у разі аварії або витоку.

Автоматичне шифрування резервних копій – забезпечує захист від несанкціонованого доступу до резервних даних.

Тестування процесу відновлення – перевірка цілісності даних і працездатності систем після аварій.

Системи моніторингу та аудиту

SIEM-системи (Security Information and Event Management) – збір, кореляція та аналіз подій безпеки.

Журналювання доступу та змін даних – контроль операцій користувачів із персональними даними.

Системи DLP (Data Loss Prevention) – контроль витоку конфіденційної інформації через зовнішні канали.

3.3 Проведення експерименту (апробації) та аналіз одержаних результатів

Експериментальна апробація розробленої методики захисту персональних даних спрямована на перевірку ефективності комплексного підходу до забезпечення безпеки цифрових даних у реальному середовищі

організації. Експеримент включав практичне впровадження заходів захисту на локальному та мережевому рівнях та оцінку їх впливу на безпеку та доступність персональної інформації.

1. Підготовчий етап

Перед проведенням експерименту були виконані такі підготовчі заходи:

1. Інвентаризація інформаційних ресурсів – визначення всіх баз даних, робочих станцій, серверів та каналів обробки персональних даних.

2. Класифікація даних – розподіл персональної інформації за рівнем критичності та чутливості.

3. Встановлення контрольних показників – визначення критеріїв оцінки ефективності методики:

рівень несанкціонованого доступу;

цілісність даних;

доступність інформаційних систем;

швидкість реагування на інциденти.

4. Визначення сценаріїв тестування – створення умов, що моделюють потенційні загрози: спроби несанкціонованого доступу, витоку даних, атаки на мережеву інфраструктуру.

2. Проведення експерименту

Локальний рівень захисту

На робочих станціях співробітників були впроваджені:

антивірусне ПЗ та антишпигунські системи;

шифрування локальних дисків (BitLocker);

багатофакторна автентифікація;

контроль доступу за ролями та обмеження прав користувачів.

Результати тестування локального рівня:

усі спроби несанкціонованого доступу були зафіксовані та заблоковані;

шифрування забезпечило захист конфіденційних файлів при спробі копіювання на зовнішні носії;

багатофакторна автентифікація знизила ризик компрометації облікових записів.

Мережевий рівень захисту

На мережевому рівні впроваджено:

сегментацію мережі за VLAN;

міжмережеві екрани для контролю вхідного та вихідного трафіку;

захищені VPN-канали для віддаленого доступу;

IDS/IPS-систему для моніторингу мережевих атак.

Результати тестування мережевого рівня:

всі спроби несанкціонованого доступу ззовні були успішно заблоковані;

сегментація мережі обмежила поширення потенційних загроз між підсистемами;

система IDS/IPS виявила симульовані атаки на сервери баз даних;

передача даних через VPN виявилась безпечною, втрат чи витоку інформації не зафіксовано.

Резервне копіювання та відновлення

Створено регулярні резервні копії критичних баз даних;

Виконано тестове відновлення даних для перевірки працездатності системи.

Результати:

дані успішно відновлені без втрати цілісності;

час відновлення відповідав встановленим нормам доступності;

шифрування резервних копій забезпечило їх захист від несанкціонованого доступу.

Журналювання та аудит

Усі операції з персональними даними журналювались;

Проведено аналіз логів на предмет спроб порушення політик безпеки.

Результати:

виявлено та задокументовано декілька потенційних порушень доступу;

аудит показав, що система контролю дозволяє відслідковувати дії користувачів і оперативно реагувати на інциденти.

Аналіз одержаних результатів

Після проведення апробації було встановлено:

1. Розроблена методика забезпечує багаторівневий захист персональних даних і ефективно протидіє основним типам загроз.

2. Найвищу ефективність показали шифрування даних, багатофакторна автентифікація та сегментація мережі.

3. Резервне копіювання та тестове відновлення підтвердили здатність організації відновлювати інформацію після потенційних інцидентів.

4. Журналювання та аудит дозволили оперативно виявляти порушення та відслідковувати дії користувачів, що підвищує загальний рівень контролю.

5. Виявлені невеликі недоліки (наприклад, відсутність автоматичного моніторингу оновлень ПЗ на робочих станціях) стали підставою для рекомендацій щодо подальшого вдосконалення методики.

Висновки до третього розділу

У третьому розділі дипломної роботи проведено комплексну апробацію розробленої методики захисту персональних даних у цифровому середовищі організації, що дозволило перевірити її практичну ефективність та виявити основні переваги і потенційні недоліки при реальному використанні. На підставі проведених досліджень та експериментальної апробації можна зробити такі розширені висновки:

Цифрове середовище організації включає локальні робочі станції, серверну інфраструктуру, мережеві підсистеми та канали передачі даних, а також зовнішні інтеграції із державними та фінансовими сервісами.

Вхідні персональні дані охоплюють ідентифікаційні, контактні, соціально-економічні, професійні та спеціальні категорії даних (медичні та біометричні).

Великий обсяг та різнорідність оброблюваної інформації вимагають багаторівневого та системного підходу до забезпечення конфіденційності, цілісності та доступності даних.

Систематизація даних дозволила ідентифікувати критичні точки: робочі станції співробітників, сервери баз даних, канали передачі даних та резервні копії.

Виявлено ключові джерела надходження даних: паперові документи, веб-форми, електронна пошта та інтеграції з зовнішніми системами.

Аналіз каналів обробки даних показав, що найбільш уразливими є мережеві комунікації та зовнішні інтеграції, що потребує посиленого захисту на рівні мережі та серверів.

Впроваджено багаторівневу систему безпеки, що поєднує фізичні засоби контролю доступу (біометрія, замки, відеоспостереження), серверні та мережеві апаратні рішення (сервери з RAID/NAS/SAN, міжмережеві екрани, VPN) та програмні засоби (шифрування, антивіруси, системи резервного копіювання, DLP, журналювання і аудит).

Комплексне використання апаратних і програмних інструментів дозволяє забезпечити багаторівневий захист, контролювати доступ і зменшувати ризики витоку даних.

На локальному рівні**:** спроби несанкціонованого доступу до робочих станцій були успішно заблоковані, шифрування локальних дисків захистило конфіденційні файли, а багатофакторна автентифікація знизила ризик компрометації облікових записів.

На мережевому рівні: сегментація мережі, міжмережеві екрани та VPN забезпечили безпечну передачу даних; система IDS/IPS виявила та локалізувала симульовані атаки на сервери баз даних.

Резервне копіювання та відновлення підтвердили здатність системи швидко відновлювати дані без втрати цілісності, а шифрування резервних копій забезпечило їх безпеку.

Журналювання та аудит дозволили оперативно відслідковувати дії користувачів та виявляти порушення політик безпеки.

Виявлено відсутність централізованого контролю оновлень програмного забезпечення на робочих станціях;

Недостатньо автоматизоване сповіщення про потенційні загрози на мережевому рівні;

Рекомендовано посилити політики контролю доступу та впровадити регулярні навчання співробітників щодо інформаційної безпеки.

Ці недоліки не критичні, але їх усунення дозволить підвищити загальний рівень захисту персональних даних та забезпечити відповідність міжнародним стандартам інформаційної безпеки.

ВИСНОВКИ

У дипломній роботі вирішено актуальне науково-практичне завдання — обґрунтування та розроблення комплексної методики захисту персональних даних у цифровому середовищі з урахуванням сучасних кіберзагроз, вимог нормативно-правового регулювання та принципів ризик-орієнтованого управління інформаційною безпекою. Актуальність теми зумовлена стрімкою цифровізацією суспільства, поширенням хмарних сервісів, мобільних технологій і віддалених форм роботи, що суттєво розширює поверхню атак та підвищує вразливість персональних даних.

У першому розділі здійснено ґрунтовний аналіз сучасних загроз для інформаційних ресурсів систем і персональних даних. Встановлено, що найбільш поширеними загрозами є несанкціонований доступ, витоки інформації через внутрішні та зовнішні канали, шкідливе програмне забезпечення (віруси, трояни, ransomware), фішингові атаки, атаки соціальної інженерії, експлуатація вразливостей програмного забезпечення, а також цілеспрямовані мережеві атаки. Визначено, що значну частку інцидентів спричиняє людський фактор, недостатній рівень організаційних заходів безпеки та несистемний підхід до управління ризиками.

Також у першому розділі проведено аналіз сучасних методів і засобів захисту персональних даних. Розглянуто криптографічні механізми захисту інформації, багатофакторну автентифікацію, системи розмежування доступу, антивірусні рішення, між мережеві екрани, системи виявлення та запобігання вторгненням, технології резервного копіювання та відновлення даних. Виявлено, що застосування окремих засобів без інтеграції в єдину систему не забезпечує належного рівня захисту, що підтверджує необхідність розроблення цілісної методики. На основі проведеного аналізу сформульовано формалізовану постановку завдання дослідження, визначено об’єкт, предмет, мету, критерії ефективності та обмеження, що дозволило структурувати подальшу наукову роботу.

У другому розділі розроблено комплексну методику захисту персональних даних у цифровому середовищі, що базується на принципах системності, багаторівневості та ризик-орієнтованого підходу. Проведено оцінювання ризиків шляхом ідентифікації інформаційних активів, визначення потенційних загроз і вразливостей, оцінювання ймовірності їх реалізації та можливих наслідків. Запропоновано модель визначення рівня ризику та критерії прийнятності ризиків, що дозволяє обґрунтовано приймати управлінські рішення щодо впровадження заходів захисту.

У межах методики визначено інструментарій захисту персональних даних на локальному рівні, що включає механізми автентифікації та авторизації користувачів, шифрування даних на носіях, політики безпечного налаштування робочих станцій, використання антивірусного програмного забезпечення, контроль використання зовнішніх носіїв інформації та аудит дій користувачів. На мережному рівні запропоновано використання між мережевих екранів, VPN-технологій для захищеного віддаленого доступу, систем виявлення та запобігання вторгненням, сегментації мережі, моніторингу мережевої активності та централізованого журналювання подій безпеки.

Розроблено структурну схему методики, яка відображає послідовність і взаємозв’язок її етапів: інвентаризація активів, аналіз загроз і вразливостей, оцінювання ризиків, вибір та впровадження засобів захисту, моніторинг, аудит і періодичний перегляд ефективності заходів. Такий підхід забезпечує адаптивність методики до змін у цифровому середовищі та дозволяє масштабувати її відповідно до потреб організації.

У третьому розділі проведено апробацію розробленої методики в умовах конкретного цифрового середовища. Здійснено аналіз вхідних даних, визначено особливості інформаційної інфраструктури та рівень початкової захищеності. Сформовано перелік апаратних і програмних засобів захисту, необхідних для реалізації запропонованої методики. У ході експериментальної перевірки здійснено впровадження комплексу заходів і проведено оцінювання їх ефективності за визначеними критеріями.

Результати апробації продемонстрували зниження рівня інформаційних ризиків, підвищення стійкості системи до типових кіберзагроз, зменшення ймовірності несанкціонованого доступу до персональних даних, а також покращення контролю за обробкою та зберіганням інформації. Отримані результати підтвердили доцільність застосування ризик-орієнтованого підходу та ефективність комплексного поєднання організаційних, технічних і програмних заходів захисту.

Практичне значення одержаних результатів полягає в можливості використання розробленої методики в діяльності підприємств, установ та організацій різних форм власності для підвищення рівня захисту персональних даних у цифровому середовищі. Методика може бути адаптована з урахуванням масштабів організації, специфіки її інформаційної інфраструктури та вимог чинного законодавства у сфері захисту інформації.

Таким чином, мету дипломної роботи досягнуто, поставлені завдання виконано повністю, а отримані результати мають теоретичну новизну та практичну цінність. Подальші дослідження можуть бути спрямовані на автоматизацію процесів оцінювання ризиків, інтеграцію методики з міжнародними стандартами управління інформаційною безпекою та вдосконалення механізмів реагування на кіберінциденти в умовах постійної трансформації цифрового середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Національну програму інформатизації: Закон України № 74/98-ВР від 04.02.1998 // Відомості Верховної Ради України. — 1998. — № 27-28. — ст. 181.

2. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України: автореф. дис. д-ра політ. наук. — Одеса, 2005. — 36 с.

3. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп'ютерних мережах. — К.: Наукова думка, 2009. — 295 с.

4. Хорошко В. О., Чекатков А. А. Методи та засоби захисту інформації: Підручник. — К.: Юніор, 2003. — 504 с.

5. Юдін О. К., Фролов О. В., Мацук З. В. Кібербезпека: світові тенденції та виклики. — К.: НАУ, 2013. — 432 с.

6. Гребенников В. В. Криптографічні методи захисту інформації: Навчальний посібник. — К.: НаУКМА, 2010. — 180 с.

7. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: Підручник. — К.: ДУТ, 2015. — 288 с.

8. Дубчак П. В. Побудова комплексних систем захисту інформації: Навчальний посібник. — Житомир: ЖВІ НАУ, 2012. — 156 с.

9. Беляков К. І. Інформаційне право: Навчальний посібник. — К.: КНТ, 2006. — 400 с.

10. Брижко В. М. Захист персональних даних: міжнародні стандарти та українське законодавство. — К.: КНТ, 2010. — 252 с.

11. Скулиш М. А. Методи оцінки ризиків інформаційної безпеки в телекомунікаційних системах. — К.: КНУ, 2014. — 210 с.