Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: Методи захисту особистих даних працівників на підприємстві

Виконавець: студента IV курсу, групи КБ-42

_____ **Нікіта КРЕЖЕНСТОВСЬКИЙ**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Олександр ЛАПТЄВ	

Нормоконтроль	Олександр ТОРОШАНКО	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студента **КБ-42** (група) **Креженстовського Нікіти Романовича** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Методи захисту особистих даних працівників на підприємстві

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Методи та алгоритми захисту особистих даних

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теорією захисту даних, вразливостями з боку безпеки даних. Аналіз методів захисту особистих даних працівників на підприємстві. Визначення недоліків та проблем практики захисту особистих даних на підприємствах. Вироблення розробки методів та стратегій захисту особистих даних працівників на підприємстві.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розробка методів та стратегій захисту особистих даних працівників на підприємстві.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Олександр ЛАПТЄВ (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Нікіта КРЕЖЕНСТОВСЬКИЙ (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 22.01.2023	*виконано*
2	Аналіз літератури	29.01.2023 – 11.02.2023	*виконано*
3	Обґрунтування вибору рішення	12.02.2023 – 15.02.2023	*виконано*
4	Поняття особистих даних та їх класифікація	16.02.2023 – 04.03.2023	*виконано*
5	Аналіз методів захисту особистих даних працівників на підприємстві	05.03.2023 – 21.03.2023	*виконано*
6	Визначення недоліків та проблем практики захисту особистих даних на підприємствах	22.03.2023 – 08.04.2023	*виконано*
7	Вироблення розробки методів та стратегій захисту особистих даних працівників на підприємстві	09.04.2023 – 10.05.2023	*виконано*
8	Оформлення пояснювальної записки	11.05.2023 – 27.05.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Олександр ЛАПТЄВ (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Нікіта КРЕЖЕНСТОВСЬКИЙ (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 67 сторінок основного тексту та 5 таблиць. Список використаних джерел містить 27 найменувань і займає 3 сторінки.

Метою дипломної роботи є розробка рекомендацій щодо захисту особистих даних працівників на підприємстві.

Методи дослідження кваліфікаційної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння;

Об'єктом дослідження є процес захисту особистих даних на підприємстві

Предметом дослідження в даній роботі є методи та стратегії захисту особистих даних працівників на підприємстві.

вивчення та узагальнення вітчизняної і зарубіжної практики. У роботі проаналізована існуюча література з теорії захисту персональних даних, виконаний аналіз документів, порівняння, вивчення та узагальнення вітчизняної і зарубіжної практики з теми захисту персональних даних, розроблено рекомендації з оцінювання методів та стратегій захисту персональних даних на підприємстві.

Розроблені рекомендації призначені для підприємств, що хочуть забезпечити безпеку своїх персональних даних на підприємстві.

Ключові слова: Захист персональних даних, безпека персональних даних на підприємстві, оцінка розроблених методів , система контроля доступу.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AES – Advanced Encryption Standard

GDPR - General Data Protection Regulation

IT – Information Technology

VPN – Virtual Private Network

АІС – Автоматизована інформаційна система

ІКТ – Інформаційно-комунікаційні технології

ПЗ – Програмне забезпечення

ЕОМ – Електронно-обчислювальна машина

ІС – Інформаційні системи

ЛОМ — локальна обчислювальна мережа

ПД – Персональні дані

СКУД – Система контроля доступу

СЗІ — Служба захисту інформації

ЦОД - Центр обробки даних

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі зберігання та обробка особистих даних стали складними та надзвичайно важливими завданнями для будь-якого підприємства. Особисті дані працівників на підприємстві містять чутливу інформацію, яка може бути використана для різних цілей, включаючи зловживання, шахрайство та порушення приватності. Це відкриває можливості для різних загроз, таких як крадіжка даних, розкриття конфіденційної інформації або надмірне збирання даних, що може призвести до суттєвих наслідків для працівників та підприємства в цілому.

У зв'язку з цим, тема захисту особистих даних працівників на підприємстві є дуже актуальною та потребує уваги від науковців та практиків. Дослідження методів захисту особистих даних на підприємстві допоможе зрозуміти проблеми та визначити оптимальні методи та стратегії захисту даних.

Метою дипломної роботи є розробка рекомендацій щодо захисту особистих даних працівників на підприємстві.

Для досягнення поставленої мети дипломної роботи необхідно виконати наступні завдання:

1. Дослідити аспекти захисту особистих даних на підприємстві, включаючи класифікацію особистих даних, законодавчі акти та стандарти.
2. Провести аналіз практики захисту особистих даних на підприємствах, визначити недоліки та проблеми в практиці захисту даних.
3. Розробити рекомендації щодо захисту особистих даних працівників на підприємстві та оцінити їх ефективність.

Об'єкт дослідження - захист особистих даних працівників на підприємстві.

Предмет дослідження - методи та стратегії захисту особистих даних працівників на підприємстві.

Методи дослідження:

1. Аналіз наукової літератури, законодавчих актів та стандартів щодо захисту особистих даних на підприємстві.
2. Експертні опитування та інтерв'ю з фахівцями в галузі захисту даних.
3. Аналіз практичних випадків порушення безпеки даних на підприємствах.

Практична цінність. Результати даної дипломної роботи матимуть практичне значення для підприємств, що працюють з особистими даними своїх працівників. Впровадження розроблених методів та стратегій захисту даних дозволить зменшити ризики порушення безпеки даних, забезпечити відповідність законодавству та захист прав працівників щодо обробки їхньої особистої інформації. Крім того, дана робота може стати основою для подальших досліджень у сфері захисту особистих даних та сприяти розвитку інформаційної безпеки на підприємствах.

РОЗДІЛ 1
АНАЛІЗ АСПЕКТІВ ЗАХИСТУ ОСОБИСТИХ ДАНИХ НА ПІДПРИЄМСТВІ

1.1. Поняття особистих даних та їх класифікація

У сучасному динамічному світі швидкого розвитку та змін суспільство все більше використовує інформацію про окремих людей, людей загалом, громадян націй тощо. Під час взаємодії людини з навколишнім світом відбувається обмін інформацією, що призводить до використання та обробки персональних даних, зокрема про її ім’я та по батькові, місце проживання, стан здоров’я, номер мобільного телефону, кредит. історія, страховка . Особисті майнові та немайнові права дозволяють виділити та ідентифікувати конкретну фізичну особу серед інших.

Особисті дані відносяться до інформації, яка може бути ідентифікована або пов'язана з конкретною фізичною особою. Забезпечення відповідного рівня захисту особистих даних є надзвичайно важливим, особливо в контексті зростаючої кількості кіберзлочинів і порушень приватності.

Особисті дані можна класифікувати залежно від різних аспектів, включаючи їх тип, чутливість, джерело, обробку та інші фактори. Загальні типи особистих даних включають інформацію про ідентифікацію (наприклад, ім'я, адреса, номер соціального страхування), контактні дані (телефон, електронна пошта), фінансову і банківську інформацію, медичні записи, біометричні дані, інформацію про геолокацію та інші.

Класифікація особистих даних також може базуватися на їх чутливості та ризику. Чутлива інформація включає дані, які можуть призвести до дискримінації, шкоди або недоброзичливих дій проти особи, такі як расова або етнічна приналежність, політичні переконання, релігійна переконаність, стан здоров'я, сексуальна орієнтація та інші. Ризик особистих даних визначається можливістю

незаконного доступу, втрати, зміни чи розголошення такої інформації. Детальне розуміння поняття особистих даних та їх класифікації є ключовим для розробки та впровадження ефективних стратегій та заходів щодо захисту особистих даних на підприємстві. Відповідна класифікація дозволяє визначити рівень захисту, необхідний для різних типів особистих даних, і прийняти відповідні заходи для запобігання порушенням та забезпечення конфіденційності, цілісності та доступності цих даних.

Для кращого розуміння теми проведемо порівняння різних визначень до поняття «особисті дані» в таблиці 1.1.

Таблиця 1.1

Визначення поняття «особисті дані» з точки зору різних дослідників та науковців

Науковець	Визначення «особисті дані»
Михайло Петренко	Особисті дані - це будь-яка інформація, яка безпосередньо або опосередковано стосується конкретної особи, ідентифікованої або ідентифікованої. Вона може включати такі дані, як ім'я, адресу, номер телефону, електронну пошту, фінансову інформацію, медичні записи, інформацію про геолокацію та інші.
Олексій Іваненко	Особисті дані - це інформація, яка дозволяє безпосередньо або опосередковано ідентифікувати окрему особу. Вона може включати такі дані, як ім'я, адреса, номер телефону, соціальний номер, фізичні характеристики тощо. Важливо захищати ці дані, щоб забезпечити приватність і недопущення незаконного використання.
Ірина Семененко	Особисті дані - це будь-яка інформація, яка може бути ідентифікована або пов'язана з конкретною особою. Вона включає в себе дані, які використовуються для ідентифікації особи, такі як ім'я, адреса, номер соціального страхування, а також іншу

	інформацію, яка пов'язана з особою, таку як медичні записи, фінансова інформація, деталі транзакцій та багато іншого.

Ця таблиця містить визначення поняття "Особисті дані" від трьох українських вчених: Михайла Петренка, Олексія Іваненка та Ірини Семененко. Кожен вчений надає своє розуміння особистих даних, вказуючи, що це інформація, яка пов'язана з конкретною особою і може включати різні типи даних, такі як ім'я, адреса, номер телефону, соціальний номер, фізичні характеристики, медичні записи, фінансова інформація тощо. Вони також підкреслюють важливість захисту цих даних для забезпечення приватності та недопущення незаконного використання.

Розвиток інформаційних технологій та засобів обробки даних викликає необхідність посилення правового захисту прав особи від несанкціонованої автоматичної обробки та використання даних. Вищезазначений зміст закріплено Конституцією України від 28 червня 1996 року Верховною Радою України.

Відповідно до ст. 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Конфіденційну інформацію про осіб забороняється збирати, зберігати, використовувати та поширювати без згоди особи, крім випадків, передбачених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Для реалізації прав, встановлених ст. Формування статті 32 Конституції України та механізм її застосування 1 червня 2010 року Верховна Рада України прийняла Закон України «Про захист персональних даних».

Зміст Закону України «Про захист персональних даних» чітко визначає суспільні відносини, пов’язані із захистом та обробкою персональних даних, і спрямований на захист основних прав і свобод людини і громадянина, особливо права не втручатися в особисте життя, пов’язане з обробка персональних даних. Сфера дії Закону поширюється на обробку персональних даних, що здійснюється повністю або частково з використанням автоматизованих засобів, а також обробку персональних

даних, які містяться або призначені для внесення до картотеки, з використанням неавтоматизованих засобів.

Як видно зі структури цього закону, він містить 30 статей і має термінологічне наповнення, щоб ми могли зрозуміти спеціальну термінологію. Серед них особливої уваги заслуговує запропоноване визначення персональних даних. Відповідно до ст. Статтею 2 Закону України «Про захист персональних даних» визначено, що «персональними даними є відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована»[3].

Для визначення персональних даних як правової категорії необхідно звернути увагу на трактування науковцями понять «категорія» та «правова категорія».

Тому О. О. Селіванова розглядає термін «категорія» як найзагальніше базове поняття, що відображає сутність, закономірні зв'язки та відношення об'єктів пізнання та дослідження [7, с.716].

На думку Н. І. Панова, «правова категорія» є найбільш загальним, фундаментальним і глибоким правовим поняттям і є межею наукового узагальнення як у певній галузі правових знань, так і в усій юридичній та юридичній практиці [8, с. 18]. Отже, виходячи з вищевикладеного, можна зазначити, що з прийняттям в Україні «Закону про захист персональних даних» у національному законодавстві сформувалася «правова категорія» «персональні дані».

У Конвенції Європейської Комісії № 108 від 28 січня 1981 року про захист осіб у зв'язку з автоматизованою обробкою персональних даних вперше було надано визначення персональних даних, у якому зазначено, що «персональні дані — це інформація, що стосується конкретної особи». або такі особи можуть бути ідентифіковані» [9].

Сьогодні Конвенція РЄ 1981 року продовжує функціонувати як основний документ, що визначає принципи міжнародних прав і свобод людини щодо захисту персональних даних і є основним світовим правовим стандартом у сфері захисту персональних даних.

Розглянувши визначення, запропоновані у вітчизняному законодавстві, та порівнявши їх із визначеннями, викладеними у вищезазначених конвенціях, можна зробити висновок, що європейське розуміння персональних даних поширюється на Закон України «Про захист персональних даних» 2010 року.

Згодом Європейський Союз прийняв Директиву 95/46/ЄС Європейського Парламенту та Ради від 24 жовтня 1995 року про захист фізичних осіб під час обробки персональних даних та про вільний рух таких даних. Відповідно до ст. Стаття 2 Директиви 95/46/ЄС «Персональні дані — це будь-яка інформація, що стосується ідентифікованої або ідентифікованої фізичної особи (суб'єкта даних); ідентифікована особа — це особа, яку можна ідентифікувати прямо чи опосередковано, зокрема за ідентифікаційним кодом або одним або більш притаманні чинники фізичного, фізіологічного, психологічного, економічного, культурного чи соціального аспектів його особистості»[10].

У Повідомленні Європейської Комісії № COM (2010) 609 від 4 листопада 2010 р., адресованому Європейському Парламенту, Раді Європейського Союзу, Економічно-соціальному комітету та Комітету регіонів Європейського Союзу «Захист персональних даних у Європейський Союз» зазначає, що термін «персональні дані» призначений для охоплення всієї інформації, що стосується можливості ідентифікації або прямо чи опосередковано ідентифікації особи. Щоб визначити, чи можна ідентифікувати особу, слід розглянути всі засоби, за допомогою яких власник персональних даних або будь-яка інша особа може бути використана для ідентифікації цієї особи [11].

Відповідно до мотивувальної частини Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012 суд зазначив, що «відомостями про особисте та сімейне життя особи (персональні дані про неї) є будь-які відомості про фізична особа або сукупність відомостей, які ідентифікують або можуть бути конкретно ідентифіковані, а саме: національність, освіта, сімейний стан, віросповідання, стан здоров'я, адреса, дата та місце народження, місце проживання та перебування тощо члени сім'ї), а також відомості про події та явища, що відбуваються і відбуваються в

сімейному, суспільному, професійному, господарському та інше, за винятком даних, пов’язаних із здійсненням повноважень особами, які виконують відповідні посади в земських функціях»[12].

Крім конституційних тлумачень персональних даних, існують такі вчених, які дають теоретичне осмислення такої правової категорії як персональні дані. З них заслуговує на увагу думка М. І. Саєнка, який зазначає, що «під поняттям персональних даних слід розуміти дані про живу особу, які ідентифіковані або можуть бути ідентифіковані за цими даними або за додатковими даними. доступні особі дані, що містять вираження цієї особи та вказівку на конкретну мету чи плани цієї особи особою, яка контролює дані, або іншими» [6, с.103].

Науковець В. Брижко стверджує, що «персональні дані – це індивідуальна інформація або сукупність ідентифікованої чи ідентифікованої такої інформації про фізичну особу» [3, с. 168]. Це визначення поширюється на Закон України «Про захист персональних даних» від 16 березня 2006 року та приймається в цілому. Пізніше в Законі України «Про захист персональних даних» від 1 червня 2010 року було встановлено, що «персональними даними є відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована».

Науковець Г. Виноградова стверджує, що «персональні дані – це сукупність зафіксованих або оприлюднених відомостей про фізичну особу» [4, с.176].

Проте, за словами О. Бреля, визначення персональних даних, наведене в Законі України «Про захист персональних даних», хоч і відповідає міжнародній практиці, не є вичерпним і не передбачає чітких критеріїв, за якими дані фізичних осіб можуть вважатися персональними [5, с. 220].

Отже, проаналізувавши судову практику та думки науковців, можна зазначити, що запропонований у Законі України «Про захист персональних даних» термін «персональні дані» базується на принципі ідентифікації даних фізичних осіб.

Під ідентифікацією (від лат. identifico – «ототожнюю») розуміють виділення індивідуально визначеного об’єкта з-поміж багатьох подібних, однорідних об’єктів на основі достовірно встановленої системи ідентифікаційних ознак [13, с. 211].

Означена ідентифікація здійснюється за низкою критеріїв, чітко визначених у чинному законодавстві України, що підтверджує думку вченого О. Бреля про те, що в чинному законодавстві не встановлено вичерпного переліку, який би вказував, які дані про природну особу можна вважати окремою особою. Так, вона їм не належить.

Крім того, для визначення та удосконалення персональних даних як правової категорії слід зазначити, що в суспільстві можна спостерігати, що персональні дані використовуються без згоди суб'єкта персональних даних. Яскравим прикладом є використання персональних даних під час виборів та формування списків виборців, яке здійснюється без згоди володільців таких персональних даних.

Є багато прикладів цього, особливо в медичній сфері, де використовуються особисті дані пацієнтів, особливо дані історії хвороби чи інші дані. У сучасних умовах ми можемо використовувати персональні дані з публічних реєстрів, таких як Реєстр судових рішень чи Єдиний реєстр державних декларацій, ми можемо використовувати персональні дані про майновий стан чи доходи суб'єкта персональних даних без його згоди.

Крім того, використання персональних даних здійснюється в судовій сфері, де відповідні дані використовуються без згоди на використання таких даних. Відповідно до основних вимог позову при складанні та поданні до суду відповідна графа для надання такої згоди відсутня.

З сайту «Реєстр судових рішень» ми отримуємо інформацію про місце проживання позивача, відповідача, прізвище, ім'я та по батькові представників сторін, ідентифікаційний номер та місцезнаходження майна. Спір знаходиться на розгляді. Ця інформація може бути використана для встановлення особи. Однак така інформація є персональними даними і може використовуватися без відповідної згоди.

Відповідно до ст. 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Забороняється збирати, зберігати, використовувати та поширювати конфіденційну інформацію про осіб без їх згоди, крім випадків, передбачених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

У цьому контексті Конституція України як вищий нормативний закон містить правові вказівки щодо збирання, зберігання, використання та поширення конфіденційної інформації про особу без згоди особи, регулюючи суспільні відносини в особистій сфері. персональні дані, призначені для їх захисту.

Відповідно до ст. Стаття 25 Закону України «Про захист персональних даних» передбачає, що у випадках, передбачених законом, чинність статей 6, 7 і 8 цього Закону може бути обмежена на необхідний термін. національної безпеки, економічного добробуту чи захисту прав і свобод суб'єктів, об'єктів чи інших персональних даних. Обробка персональних даних дозволяється, якщо положення цього Закону не застосовуються, якщо така обробка має місце: право на свободу особистого життя та самовираження. Дія цього Закону не поширюється на відносини щодо доступу до інформації в архівах репресивних органів.

Цілком логічно розуміти зарубіжну практику, що відповідна згода необхідна лише для використання конфіденційних персональних даних щодо фізичних осіб, тому вважаємо, що, окрім введення нормативно-правового переліку персональних даних до чинних законів загального та делікатного характеру, ми вважаємо, що для використання конфіденційних персональних даних щодо фізичних осіб необхідно отримати відповідну згоду. Доцільно ввести додаткову специфікацію, яка б вказувала на згоду на обробку або використання персональних даних

Дані необхідно надавати у випадках використання конфіденційних даних про фізичних осіб. Крім того, на нашу думку, під персональними даними слід розуміти інформацію або сукупність відомостей про живу фізичну особу, яка є або може бути конкретно ідентифікована

При ідентифікації враховується законодавчо встановлений поділ персональних даних.

Також хочемо розглянути класифікацію особистих даних яка є важливим аспектом в області захисту особистої інформації. Залежно від різних аспектів, таких як тип даних, чутливість, джерело, обробка та інші фактори, особисті дані можна класифікувати наступним чином:

1. За типом даних:

- Ідентифікаційні дані: інформація, що використовується для ідентифікації особи, наприклад, ім'я, адреса, номер соціального страхування тощо.
- Контактні дані: дані, що дозволяють зв'язатися з особою, такі як телефонний номер, електронна адреса тощо.
- Фінансові дані: інформація про фінансовий стан особи, включаючи банківські реквізити, кредитну історію тощо.
- Медичні дані: дані про стан здоров'я, медичні записи, лікування тощо.
- Біометричні дані: фізичні характеристики особи, які можуть бути використані для ідентифікації, наприклад, відбитки пальців, розпізнавання обличчя, голосу тощо.
- Геолокаційні дані: інформація про місцезнаходження особи, яка збирається, наприклад, через GPS, мобільний зв'язок тощо.

2. За чутливістю:

- Звичайні особисті дані: інформація, яка не вважається особливо чутливою або приватною, наприклад, контактна інформація.
- Чутливі особисті дані: інформація, яка може призвести до дискримінації, шкоди або недоброзичливих дій проти особи, така як расова або етнічна приналежність, політичні переконання, релігійна переконаність, стан здоров'я, сексуальна орієнтація тощо.

3. За джерелом:

- Прямі дані: інформація, яку особа надає самостійно, наприклад, при реєстрації на веб-сайті чи заповненні анкети.
- Посередні дані: інформація, яку збираються від сторонніх джерел, таких як партнери, соціальні мережі, публічні джерела тощо.

4. За обробкою:

- Активні дані: дані, з якими особа свідомо взаємодіє або надає, наприклад, при виконанні операцій, введенні інформації тощо.

- Пасивні дані: дані, що автоматично збираються або відстежуються, наприклад, через використання кукісів, датчиків, моніторингу активності тощо.

Ця класифікація допомагає краще розуміти різноманітні типи особистих даних та їх особливості, що є важливим для визначення належного рівня захисту та встановлення відповідних заходів забезпечення конфіденційності, цілісності та доступності цих даних.

Розглянувши поняття персональних даних як правової категорії, можна помітити, що український закон «Про захист персональних даних» приймає європейський підхід до розуміння категорій персональних даних. Проте, розглядаючи інформаційні відносини в сучасному суспільстві та використання телекомунікаційних систем і методів обробки інформації, необхідно визначити точний перелік персональних даних, розділених на загальні дані та конфіденційні дані

1.2. Методи захисту особистих даних працівників на підприємстві

Загалом, захист - це заходи, які реалізує система для контролю доступу, захисту даних (конфіденційності, цілісності, доступності), опису процесів і процедур, захисту від атак, технічної підтримки, навчання та навчання персоналу [16] . Захист персональних даних - це комплекс правових, організаційних і технічних заходів, спрямованих на запобігання протиправним діям щодо персональних даних, забезпечення їх конфіденційності та можливості доступу суб'єктів персональних даних до інформації про їх дії з персональними даними. Крім того, у Вікіпедії захист персональних даних представлено як комплекс заходів технічного, організаційного та організаційно-технічного характеру, спрямованих на захист інформації, що стосується конкретних фізичних осіб або фізичних осіб, ідентифікованих на основі такої інформації (суб’єкти особисті дані) [9].

Забезпечення захисту персональних даних у базах персональних даних покладається на володільця персональних даних. Відповідно до Закону України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI володільцем персональних даних є фізична або юридична особа, яка визначає цілі обробки персональних даних, визначає склад цих даних та порядок обробки персональних даних. для його обробки. Сторони, яких стосуються персональні дані, зобов'язані забезпечити захист цих даних від незаконної обробки, зокрема від втрати, незаконного чи випадкового знищення, а також від незаконного доступу.

Цей захист важливий з огляду на те, що власники персональних даних обробляють велику кількість персональних даних за допомогою елементів керування мережевими ресурсами в Інтернеті.

Ми вважаємо за доцільне окремо документувати такі процеси:

1) Подача резюме або CV через онлайн-сервіси самої компанії та спеціалізовані сайти (work.ua, rabora.ua та ін.) для розгляду відповідності особи вакантному робочому місці. У CV людина прагне розкрити практично всю особисту інформацію про себе, яка є легкодоступною;

2) Інтернет-соціальні опитування респондентів – навіть анонімні опитування співробітників на основі певної послідовності питань можуть безпомилково ідентифікувати людину.

При цьому може оброблятися надзвичайно широкий спектр персональних даних: від анкетних персональних даних (які водночас є інформацією про ідентифіковану особу) до інформації, яка може бути опосередковано пов'язана з особою або може бути використана в процесі для ідентифікації фізичної особи: інформація про використання платіжних карток Платіжна інформація за послуги, логіни та паролі, записи в соціальних мережах, номери телефонів, адреси електронної пошти тощо.

Підставою для використання персональних даних працівників є їх згода на обробку цих даних. На перший погляд, письмова згода суб'єкта на збір, обробку та використання персональних даних видається логічним кроком у відносинах між

працівником та керівництвом компанії. Однак реальність використання таких форм згоди наочно демонструє їхню недосконалість.

Зокрема, серед проблем, які існують у практиці звернення за згодою на обробку персональних даних працівників підприємства (і звісно клієнтів), слід звернути увагу на такі питання[18]:

1) Незамінна згода – зазвичай немає можливості змінити текст «згоди на обробку персональних даних», наприклад, обмеживши можливість передачі інформації третім особам або визначивши час після обробка персональної інформації про те, що дані повинні бути видалені;

2) Непропорційний обсяг персональних даних та її прав.

Обробка - компанії, які збирають і підтримують бази персональних даних, можуть зручно запитувати у своїх співробітників і клієнтів негайну згоду відповідно до всіх можливих правил, щоб у разі будь-яких змін у бізнес-процесах використання бази даних залишалося належним чином дозволеним;

3) Надлишковість і неможливість відслідковувати надану згоду – при замовленні товарів чи послуг (клієнти) або виконанні посадових обов'язків (працівники), пов'язаних із виконанням робіт певного характеру, особа змушена регулярно підписувати згоду на обробку своїх персональних даних. У результаті майже кожен клієнт (або працівник) отримує численні згоди на обробку персональних даних, часто з непропорційними повноваженнями щодо обробки та використання, але неможливо ідентифікувати всіх суб'єктів, які дали таку згоду;

4) Паперова бюрократія – багато підприємств витрачають час і ресурси на сумлінну розробку, оформлення та зберігання заяв про згоду на обробку персональних даних і борються за підтримку власних баз персональних даних відповідно до чинного законодавства. Проте, судячи з наведеної ситуації, такі витрати підприємств є необґрунтованими, а захист персональних даних не посилений;

5) Відсутність безпеки персональних даних – вимога підписати згоду на обробку персональних даних на практиці не запобігає їх несправедливому розповсюдженню. Наприклад, так звана «телефонна книга», де можна знайти повне

ім’я людини, адресу, номер телефону, дату народження тощо, досі залишається загальнодоступною.

До того ж використовують три групи методів захисту від вірусів:

1. Методи, засновані на аналізі вмісту файлів (включаючи файли даних і файли з кодами команд). Ця група включає сканування на наявність вірусних сигнатур, перевірку цілісності та сканування на наявність підозрілих команд.

2. Метод, заснований на моніторингу поведінки програми під час виконання програми. Ці методи полягають у записі всіх подій, які загрожують безпеці системи, які відбуваються під час фактичного виконання коду, що перевіряється, або під час його програмного моделювання.

3. Метод стандартизації порядку роботи файлів і програм. Ці методи є адміністративними заходами безпеки.

Метод сканування підписів. Для кожного нововиявленого вірусу фахівці антивірусної лабораторії проводять аналіз коду та відповідно визначають його сигнатуру. Отримані фрагменти коду поміщаються в спеціальну базу сигнатур вірусів, з якої запускається антивірусна програма. Перевагою цього методу є відносно низький рівень помилкових спрацьовувань, а основним недоліком є те, що виявити нові віруси в системі, яка не має сигнатури в базі даних антивірусної програми, просто неможливо, тому своєчасне оновлення сигнатури потрібна база даних.

Підхід до контролю цілісності заснований на тому, що будь-які несподівані та незрозумілі зміни даних на диску є підозрілими подіями, які вимагають особливої уваги з боку антивірусних систем. Віруси обов'язково залишають докази свого існування (зміни даних в існуючих (особливо системних або виконуваних) файлах, поява нових виконуваних файлів тощо). Той факт, що дані змінилися (порушення цілісності), можна легко визначити, порівнявши контрольну суму (дайджест), попередньо обчислену для початкового стану тестового коду, з контрольною сумою (дайджестом) поточного стану тестового коду. Якщо вони не збігаються, це означає, що цілісність порушена, і є вагомі причини для додаткових перевірок коду, наприклад, шляхом сканування на наявність вірусних сигнатур.

Метод сканування підозрілих команд (евристичний сканування, евристичний метод) заснований на виявленні певної кількості підозрілих команд та/або ознак підозрілих кодових послідовностей у сканованих файлах (наприклад, команда форматування жорсткого диска або бути введеним у запущений процес або функцію у виконуваному коді). Після цього робляться припущення про шкідливий характер файлу та вживаються інші заходи для його перевірки. Цей метод має хорошу швидкість дії, але часто не вдається виявити нові віруси.

Спосіб відстеження поведінки програми принципово відрізняється від згаданого раніше методу перевірки вмісту файлу. Цей метод, заснований на аналізі поведінки запущених програм, можна порівняти із затриманням злочинців «вручну» на місці злочину. Антивірусні інструменти цього типу зазвичай вимагають активної участі користувача, вимагаючи від користувачів прийняття рішень на основі великої кількості системних попереджень, значна частина яких пізніше може перетворитися на помилкові спрацьовування. Рівень хибних позитивних результатів вище певного порогу (підозра на вірус для нешкідливого файлу або відсутність шкідливого файлу) вимикає метод, і користувач може припинити реагувати на попередження або вибрати оптимістичну стратегію (дозволити всі дії з усіх програм, щоб увімкнути або вимкніть цю функцію антивіруса).

Методи захисту особистих даних працівників на підприємстві включають широкий спектр заходів, що спрямовані на забезпечення конфіденційності, цілісності та доступності цих даних. Розглянемо деякі з найпоширеніших методів захисту особистих даних працівників в таблиці 1.2

Таблиця 1.2

Методи захисту особистих даних працівників на підприємстві

Метод захисту	Опис
Аутентифікація	Використання ідентифікаційних механізмів, таких як паролі, біометричні дані або токени, для підтвердження

	ідентичності працівника перед отриманням доступу до особистих даних.
Авторизація	Встановлення прав доступу до особистих даних на основі ролей, обов'язків та рівня секретності. Це дозволяє обмежувати доступ до даних лише для вповноважених осіб.
Шифрування	Застосування криптографічних методів для захисту особистих даних від несанкціонованого доступу. Шифрування даних забезпечує їх конфіденційність під час зберігання та передачі.
Захист мережі	Використання файерволів, віртуальних приватних мереж (VPN) та інших технологій для захисту мережевого трафіку та запобігання несанкціонованому доступу до особистих даних.

продовження табл. 1.2

Резервне копіювання	Регулярне створення резервних копій особистих даних працівників для захисту від втрати або пошкодження даних, а також для можливості відновлення в разі аварійних ситуацій.
Політика заборони доступу	Встановлення правил та процедур щодо обмеження доступу до особистих даних лише для необхідних осіб та визначення санкцій за порушення цих правил.
Свідомість та навчання	Здійснення навчання працівників щодо захисту особистих даних, включаючи правила безпеки, розпізнавання

	фішингових атак та усвідомлення ризиків пов'язаних з обробкою даних.

Ці методи захисту особистих даних працівників допомагають підприємствам забезпечити високий рівень безпеки та конфіденційності особистої інформації своїх працівників. Варто зазначити, що кожне підприємство може застосовувати комбінацію цих методів, а також додаткові заходи відповідно до своїх конкретних потреб та вимог щодо захисту даних.

Програмні засоби включають такі програми, як ідентифікація користувача, контроль доступу, шифрування інформації, видалення залишкової (робочої) інформації, такої як тимчасові файли, і контроль тестування системи безпеки. Переваги програмних засобів - Універсальність, гнучкість, надійність, простота встановлення, можливості модифікації та розробки. Недоліки - обмежені можливості мережі, використання частини ресурсів файлових серверів і робочих станцій, висока чутливість до випадкових або навмисних змін, може залежати від типу комп'ютера (його апаратного забезпечення).

Рисунок 1.1 - Ієрархія програмних засобів захисту інформації

Також важливо знати про деякі питання, які виникають безпосередньо під час обробки персональних даних співробітників. По-перше, тут варто зазначити, що існує відсутність чіткого розуміння того, що є персональними даними та типів інформації про фізичну особу, які в законодавстві називаються персональними даними – законодавством України не встановлено і не може бути встановлено остаточного переліку відомостей про фізичних осіб, тобто персональних даних, з метою застосування положень Закону України «Про захист персональних даних» до різних ситуацій, у тому числі при обробці персональних даних в інформаційних базах та персональних даних. картотеки даних, ці дані можуть з'явитися в майбутньому внаслідок змін в економіці, суспільстві та інших сферах суспільного життя [19, с. 67].

Крім того, на сьогоднішній день немає належних нормативно-правових положень щодо перевірки приміщень, де обробляються персональні дані, та механізмів – сьогодні представники уповноважених органів мають право вільно заходити в будь-яке приміщення, де обробляються персональні дані (тобто майже в кожен офіс і кожну квартиру), яке зводиться до права на проведення обшуку, досі мали лише правоохоронні органи [17].

Під час обробки ними персональних даних ці дані публікуються в Інтернеті. Оскільки особисті дані є або можуть бути об'єктом автоматизованих систем обробки, люди залишають там багато даних, коли вони користуються Інтернетом. І, що найважливіше, використання даних не підлягає жодним обмеженням чи правилам, а це означає, що фактично такі дані залишаються незахищеними. Такі бази даних постійно вдосконалюються та гармонізуються, і вони все більше стосуються приватного життя людей [21].

Для захисту своїх персональних даних від неправомірних посягань особи можуть використовувати будь-які засоби, не заборонені законом.

Зокрема, у випадках неправомірної обробки персональних даних та втручання в особисте життя суб'єкти персональних даних мають право звернутися до володільця та/або розпорядника персональних даних та пред'явити розумні вимоги:

- заборона такої обробки;

- змінити свої персональні дані (якщо вони є недостовірними);

- вимагати його вилучення (знищення).

Водночас роботодавці також повинні вжити заходів щодо підвищення безпеки персональних даних працівників.

Тому багато дослідників захисту персональних даних пропонують розділити персональні дані на загальні персональні дані та конфіденційні персональні дані. Розділіть персональні дані на загальні (прізвище, ім'я, по батькові, дата та місце народження, громадянство, місце проживання) та конфіденційні персональні дані (щодо здоров'я – історія хвороби, діагноз тощо; етнічна приналежність; ставлення до релігії; ідентифікація).) Коди або номери; підписи; відбитки пальців, записи, фотографії; про суму доходу, про вклади та банківські рахунки, нерухомість, податковий статус; кредитну історію; дані про судимості та інші форми, які притягують особу до кримінальної, адміністративної чи дисциплінарна відповідальність, результати професійних іспитів тощо) передбачені європейськими стандартами.

Загалом європейське законодавство забороняє збір, зберігання, використання та поширення особливо чутливих персональних даних без згоди суб'єкта, а не всіх персональних даних загалом, як це робить вітчизняне законодавство [20, с.97] .

Підприємствам необхідно забезпечити їх надійну безпеку. Захист персональних даних – це комплекс заходів, спрямованих на запобігання протиправним діям щодо персональних даних, забезпечення їх конфіденційності та можливості доступу суб'єктів персональних даних до інформації про їх використання. З метою захисту своїх персональних даних від незаконного посягання фізичні особи можуть використовувати будь-які не заборонені законом засоби, серед яких окремо вимагати припинення обробки даних, зміну чи видалення даних тощо.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ПРАКТИКИ ЗАХИСТУ ОСОБИСТИХ ДАНИХ НА ПІДПРИЄМСТВАХ

2.1. Огляд практики захисту особистих даних на підприємствах

На сьогоднішній день існує широкий спектр рішень, включаючи шифрування даних, використання файрволів, антивірусного програмного забезпечення та інших захисних програм. Підприємства також використовують системи моніторингу, щоб виявляти незвичайну активність або можливі порушення безпеки.

Також не менш важливим аспектом є політика безпеки, яку встановлюють на підприємствах. Ці політики визначають правила і рекомендації, що стосуються збору, зберігання, обробки та передачі особистих даних. Вони також визначають процедури випадків порушення безпеки даних і вимоги до повідомлення про такі порушення. Ефективні політики безпеки враховують вимоги законодавства про захист персональних даних, такі як Загальний регламент про захист даних (GDPR) в Європейському Союзі.

Пов'язано з політиками безпеки є процедури управління доступом до даних. Підприємства розробляють і реалізують механізми контролю доступу до особистих даних, щоб забезпечити, що лише авторизовані особи мають доступ до цих даних. Це може включати встановлення різних рівнів доступу, шифрування даних, використання паролів, двофакторної аутентифікації та інших методів для підвищення безпеки.

Крім технологічних та організаційних заходів, на підприємствах також вкладають зусилля в розвиток культури безпеки даних серед своїх співробітників. Це означає проведення навчань та тренінгів з питань захисту особистих даних, свідомості про ризики та поведінки в разі підозрілого злочинного вторгнення або порушення безпеки. Підприємства також розробляють інформаційні матеріали та

політики, що наголошують на важливості збереження конфіденційності та безпеки даних.

Огляд практик захисту особистих даних на підприємствах включає аналіз різних підходів і стратегій, які успішно впроваджуються у сучасному бізнес-середовищі. Це дозволяє підприємствам забезпечити високий рівень безпеки особистих даних та довіру своїх клієнтів. Знання про ці практики стає ключовим фактором у боротьбі з ризиками порушення безпеки даних і дотриманням законодавства, що регулює захист особистих даних.

Компанії повинні запровадити технічні та організаційні заходи безпеки для забезпечення конфіденційності та цілісності персональних даних, щоб гарантувати захист даних від модифікації, втрати, передачі та несанкціонованого доступу. Усі заходи захисту даних повинні застосовуватися з найвищим ступенем захисту персональних даних. Заходи безпеки повинні бути частиною системи захисту даних. Далі я розгляну деякі з них і обговорю їх більш детально.

Першою розглянемо фізичну безпеку персональних даних. Фізична безпека персональних даних є одним із важливих аспектів захисту інформації на підприємствах. Вона відноситься до заходів, спрямованих на фізичний захист фізичних носіїв даних, приміщень та інфраструктури, що забезпечують зберігання і обробку цих даних.

Один з основних аспектів фізичної безпеки - це контроль доступу до приміщень та обладнання, де знаходяться особисті дані. Це може включати встановлення систем контролю доступу, таких як електронні ключ-карти, біометричні системи (відбитки пальців, розпізнавання обличчя) або використання фізичних замків і ключів. Такі заходи дозволяють обмежувати доступ лише авторизованим працівникам та іншим особам, яким це необхідно для виконання їх обов'язків.

Крім контролю доступу, також важливо забезпечити фізичну безпеку серверних приміщень та обладнання зберігання даних. Це може включати встановлення фізичних бар'єрів, таких як стійкі металеві шафи або кімнати з

контрольованим доступом. Додаткові заходи безпеки можуть включати використання відеоспостереження, сигналізаційних систем, систем автоматичного виявлення пожежі та інших протиаварійних систем.

Крім того, фізична безпека також вимагає належного зберігання інших фізичних носіїв даних, таких як паперові документи або носії інформації, які містять особисті дані. Це може включати використання сейфів або інших захищених місць для зберігання цих матеріалів. При утилізації фізичних носіїв даних важливо забезпечити їх безпечне знищення, наприклад, через шредери або спеціальні служби знищення документів.

Загальний підхід до фізичної безпеки полягає в поєднанні технологічних, організаційних і фізичних заходів для створення комплексної системи захисту персональних даних. Це дозволяє забезпечити надійний захист від неправомірного доступу, викрадення або фізичного пошкодження даних, що містять особисту інформацію.

Далі наведемо діаграму потоку інформації на веб-ресурсі рівня 0 щоб ґрунтовніше зрозуміти систему. Приклад декомпонізації роботи веб-ресурса зображено на наступній сторінці на рисунку 2.1 та рисунку 2.2.

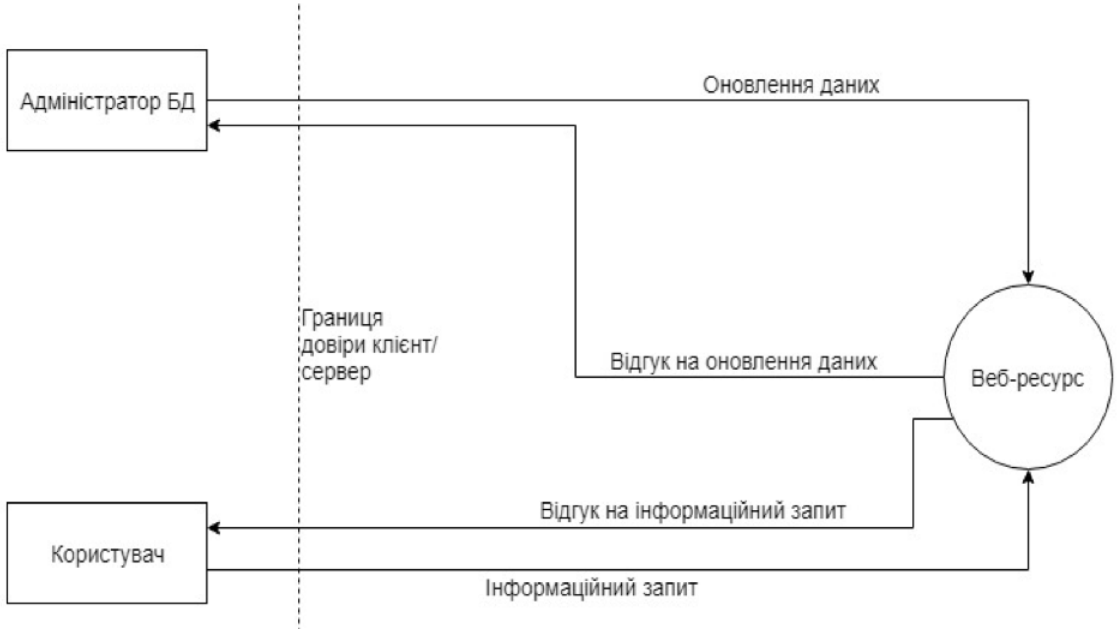

Рисунок 2.1 - Діаграма потоку даних на веб-ресурсах нульового рівня

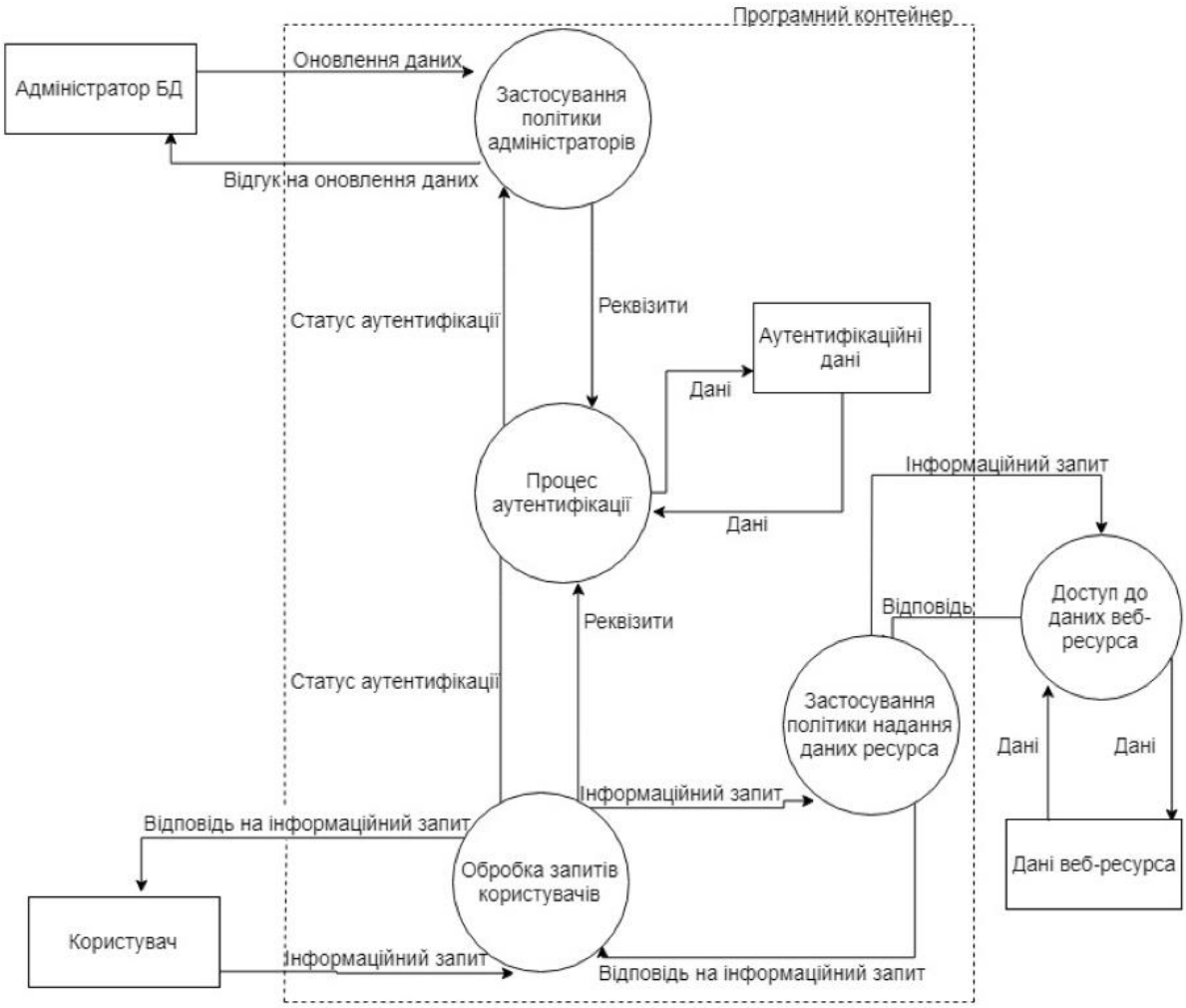

Рисунок 2.2 - Діаграма потоку даних на веб-ресурсах першого рівня

Таким чином, список основних компонентів типового веб-ресурсу виглядатиме так:

1. Адміністратор бази даних
2. Користувач
3. Інтерфейс користувача
4. Інтерфейс оновлення даних сервера
5. Сервер, на якому розташований веб-ресурс
6. Інформація про сертифікацію
7. Бізнес-логіка обробки ресурсних даних
8. Сервер бази даних
9. Ресурсні дані

10. Бізнес-логіка інтерфейсу оновлення даних ресурсу

Наступною розглянемо логічну безпеку персональних даних яка включає в себе набір заходів, спрямованих на забезпечення безпеки та конфіденційності інформації на електронних системах. Основний акцент робиться на ідентифікації та автентифікації людей або користувачів, що мають уповноваження на доступ і зміну персональних даних. Давайте розглянемо ці заходи докладніше:

1. Ідентифікація користувачів: Цей процес включає ідентифікацію особи або користувача, що намагається отримати доступ до системи. Це може включати введення ідентифікатора, такого як ім'я користувача або електронна пошта. Ідентифікатор повинен бути унікальним для кожного користувача в системі.

2. Автентифікація користувачів: Цей крок підтверджує, що особа, яка намагається отримати доступ, дійсно є власником відповідного облікового запису. Зазвичай це вимагає введення пароля або використання інших методів, таких як біометричні дані (відбитки пальців, розпізнавання обличчя) або токени доступу.

3. Керування доступом: Цей аспект визначає права доступу для кожного користувача в системі. Призначення рівнів доступу до персональних даних дозволяє обмежити права користувачів на читання, запис або зміну цих даних. Важливо забезпечити принцип найменшого доступу, де користувачі отримують лише той рівень доступу, який необхідний для виконання їх робочих обов'язків.

4. Моніторинг і аудит безпеки: Цей захід включає в себе систематичний моніторинг активності користувачів і перевірку виконання політик безпеки. Журналізування дій користувачів, аналіз логів та спостереження за подіями допомагають виявляти підозрілі або некоректні дії, які можуть загрожувати безпеці персональних даних.

5. Захист від несанкціонованого доступу: Для забезпечення безпеки персональних даних також важливо використовувати захист від несанкціонованого доступу, такий як шифрування даних. Шифрування даних допомагає захистити їх під час передачі або зберігання, у разі втрати фізичного пристрою або несанкціонованого доступу до системи.

Ці заходи щодо ідентифікації та автентифікації людей або користувачів, а також управління доступом, допомагають забезпечити логічну безпеку персональних даних, зменшити ризики несанкціонованого доступу та зберегти конфіденційність цих даних.

Проте одним із ключових аспектів безпеки персональних даних на підприємствах є програмний захист інформації. Програмний захист інформації є одним із ключових аспектів безпеки персональних даних на підприємствах.

Він охоплює широкий спектр заходів та політик, спрямованих на захист інформації в електронному вигляді, включаючи захист від несанкціонованого доступу, зламу, витоку чи зміни даних. Опишемо основні аспекти програмного захисту інформації:

1. Встановлення захисних програм та антивірусного ПЗ: Важливо мати встановлені та оновлені антивірусні програми та програми захисту від шкідливого програмного забезпечення. Ці програми дозволяють виявляти та блокувати віруси, троянські програми, шпигунське ПЗ та інші загрози, що можуть становити ризик для безпеки персональних даних.

2. Застосування механізмів шифрування: Шифрування даних є ефективним засобом захисту інформації. Застосування шифрування дозволяє перетворити дані у зашифрований формат, що забезпечує конфіденційність при передачі чи зберіганні. Для цього можна використовувати різні методи шифрування, такі як симетричне шифрування (один ключ для шифрування та розшифрування) або асиметричне шифрування (використання публічного та приватного ключів).

3. Забезпечення оновлень та патчів: Виробники програмного забезпечення регулярно випускають оновлення та патчі для своїх продуктів, які включають виправлення виявлених уразливостей і помилок. Важливо мати політику оновлення програмного забезпечення та вчасно встановлювати всі необхідні оновлення. Це допомагає запобігти використанню вразливостей програм і зберегти безпеку інформації.

4. Створення сильних паролів і багаторівневої аутентифікації: Для забезпечення безпеки інформації важливо використовувати сильні паролі, які складаються з комбінації великих і малих літер, цифр та символів. Крім того, рекомендується використовувати багаторівневу аутентифікацію, що передбачає введення додаткового фактора (наприклад, одноразового пароля, SMS-коду або біометричних даних) для підтвердження ідентичності користувача.

5. Резервне копіювання даних: Регулярне резервне копіювання даних є важливим аспектом програмного захисту інформації. Воно дозволяє відновити дані в разі випадкового видалення, втрати або виходу з ладу обладнання. Резервні копії можуть бути збережені на зовнішніх носіях, хмарних сховищах або інших безпечних медіа.

6. Встановлення прав доступу: Важливо належним чином налаштувати права доступу до програм та баз даних. Кожен користувач повинен мати обмежений доступ лише до тих функцій і даних, які необхідні для виконання його робочих обов'язків. Забезпечення принципу найменшого доступу допомагає уникнути несанкціонованого доступу та зменшити ризики витоку інформації.

7. Контроль і моніторинг активності користувачів: Для забезпечення безпеки інформації важливо вести контроль і моніторинг активності користувачів у системі. Це включає відстеження спроб незаконного доступу, моніторинг використання привілеїв, контроль змін в інформаційних системах та аналіз лог-файлів. Ці заходи дозволяють вчасно виявляти підозрілі дії та реагувати на них.

Програмний захист інформації є необхідною складовою безпеки персональних даних на підприємствах. Правильно реалізований програмний захист допомагає уникнути несанкціонованого доступу, зламу та витоку даних, забезпечує конфіденційність та цілісність інформації, а також сприяє виконанню вимог законодавства щодо захисту особистих даних.

Не менш важливим є шифрування персональних даних який є важливим заходом для забезпечення їх цілісності та конфіденційності у системі захисту даних.

Воно включає в себе впровадження та використання алгоритмів шифрування, ключів, паролів та інших заходів захисту. Давайте розглянемо цей процес детальніше:

1. Алгоритми шифрування: Для шифрування персональних даних використовуються різні алгоритми, такі як AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), DES (Data Encryption Standard) та інші. Ці алгоритми дозволяють перетворити звичайний текст (незашифрований) у шифрований текст, що є незрозумілим без використання правильного ключа або пароля.

2. Ключі шифрування: Шифрування базується на використанні ключів, які визначаються унікальними послідовностями бітів. Ключі використовуються для шифрування та розшифрування даних. Існує два основних типи ключів: симетричні та асиметричні.

- Симетричне шифрування використовує один ключ для обох процесів шифрування та розшифрування. Цей ключ повинен бути обмінений між відправником і одержувачем даних, і це вимагає взаємодії із засобами безпеки для збереження конфіденційності ключа.

- Асиметричне шифрування використовує пару ключів: публічний та приватний ключі. Публічний ключ використовується для шифрування даних, а приватний ключ - для розшифрування. Публічний ключ може бути відкритим для всіх, тоді як приватний ключ повинен бути захищений і відомий тільки власнику.

3. Паролі та ідентифікація: Для забезпечення доступу до зашифрованих даних використовуються паролі та процес ідентифікації користувача. Паролі повинні бути довгими, складними та унікальними для кожного користувача або системи. При введенні паролю, відбувається процес автентифікації, який перевіряє, чи користувач є вповноваженим на доступ до захищених даних.

4. Заходи захисту: Крім шифрування та ключів, важливо вживати інші заходи захисту, такі як контроль доступу до ключів, використання двофакторної аутентифікації, встановлення політик паролів та механізмів складних шифрів. Для забезпечення конфіденційності та цілісності даних також можуть використовуватися електронні підписи та цифрові сертифікати.

Впровадження та використання алгоритмів шифрування, ключів, паролів та конкретних заходів захисту є необхідними для забезпечення цілісності та конфіденційності конфіденційних персональних даних у системі захисту даних. Вони дозволяють попереджати несанкціонований доступ до даних та забезпечують їх безпеку під час передачі та зберігання.

В міжнародному стандарті ISO 27032 базується на загальних критеріях безпеки інформаційних технологій (Common Criteria) і на цій основі встановлює вимоги до рівнів відповідності GDPR. Відповідно до стандарту, концепція безпеки даних та їх передачі на веб-ресурсах реалізується за схемою, наведеною на рисунку 2.4. Безпека стосується захисту персональних даних користувачів інформаційних систем (веб-додатків) від можливих загроз. [2]

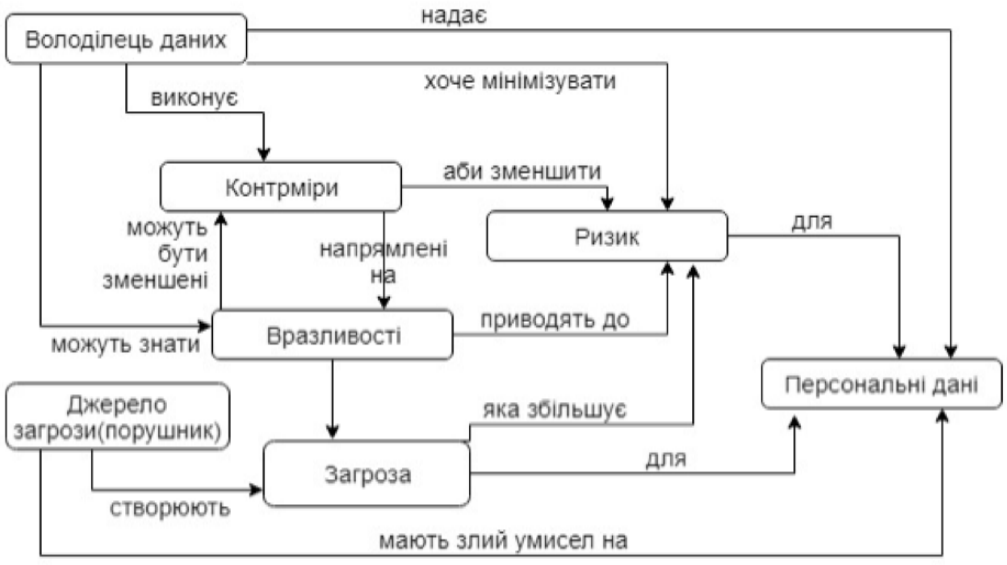

Рисунок 2.3 - Поняття безпеки даних та їх зв’язок з ISO

Мережева модель захисту даних є логічною моделлю даних, яка розширює ієрархічний підхід та використовує сувору математичну теорію для опису структурних, цілісних та обробних аспектів даних в мережевих базах даних.

Основною ідеєю мережевої моделі є здатність використовувати зв'язки між даними для організації їх у вигляді мережі. Це розширення ієрархічного підходу, в

якому дані організовані у вигляді дерева з батьківськими та дочірніми вузлами. У мережевій моделі дані можуть мати багато батьківських та дочірніх вузлів, що дозволяє більш гнучку організацію даних та відображення зв'язків між ними.

Основними поняттями в мережевій моделі є "сутність" і "відношення". Сутність представляє окремий об'єкт або елемент даних, наприклад, користувач, продукт, замовлення тощо. Відношення визначає зв'язок між сутностями та визначає структуру даних в мережевій базі даних. Відношення може мати багато-до-багатьох зв'язок, що дозволяє зв'язувати багато сутностей між собою.

Мережева модель також включає поняття "типу запису" або "схеми". Тип запису визначає структуру даних для кожної сутності та відношення. Він описує поля даних, їх типи та зв'язки з іншими типами записів.

Один з ключових аспектів мережевої моделі - це забезпечення цілісності даних. Це досягається за допомогою ієрархічної структури, яка дозволяє обмежити доступ до даних тільки через відповідні зв'язки. Таким чином, забезпечується контроль доступу та збереження цілісності даних.

У мережевій моделі захист даних зазвичай забезпечується за допомогою доступових прав доступу до вузлів та зв'язків між ними. Це означає, що користувачі мають визначені права доступу до конкретних сутностей та відношень. Наприклад, деякі сутності можуть бути доступними для перегляду лише для певних користувачів або редагування може бути дозволено лише певним групам користувачів.

Загалом, мережева модель захисту даних є математичною теорією, що дозволяє описати структурні, цілісні та обробні аспекти даних у мережевих базах даних. Вона надає гнучкість у відображенні зв'язків між даними та забезпечує контроль доступу до даних для забезпечення їх безпеки та цілісності. Розглянемо практику застосування захисту особистих даних на прикладі відомих підприємств (табл. 2.1).

Таблиця 2.1

Практика застосування захисту особистих даних на прикладах відомих підприємств

Назва компанії	Опис практики впровадження захисту особистих даних
Google	активно працює над захистом особистих даних своїх користувачів. Вони використовують широкий спектр заходів, включаючи шифрування даних під час передачі та збереження, двофакторну аутентифікацію для підвищення безпеки облікових записів та механізми контролю доступу до особистих даних.
Apple	приділяє велику увагу захисту особистих даних своїх користувачів. Вони використовують шифрування даних на пристроях, включаючи iPhone та MacBook, що дозволяє зберігати дані в зашифрованому вигляді. Крім того, вони мають строгі політики конфіденційності та контролю доступу до особистих даних, що забезпечує високий рівень безпеки.
Amazon	провідний постачальник хмарних послуг, використовує високі стандарти захисту особистих даних. Вони пропонують широкий спектр сервісів забезпечення безпеки, включаючи шифрування даних, впровадження механізмів контролю доступу та аудиту, а також фізичну безпеку дата-центрів.
Microsoft	забезпечує захист особистих даних своїх користувачів через шифрування даних, використання механізмів аутентифікації та авторизації, а також строгі політики безпеки. Вони надають можливості для управління доступом до даних та контролюють права доступу користувачів.

Ці приклади демонструють, що відомі підприємства докладають значних зусиль для забезпечення безпеки та конфіденційності особистих даних своїх користувачів. Вони використовують комплексний підхід, включаючи шифрування, механізми автентифікації, контроль доступу та політики безпеки, щоб забезпечити високий рівень захисту даних.

Нижче наведена таблиця з сильними та слабкими сторонами захисту інформації на прикладі відомих підприємств: Google, Apple, Amazon і Microsoft. Ця таблиця надає загальний огляд, і варто зазначити, що заходи захисту можуть змінюватися з часом, оскільки компанії постійно покращують свої практики.

Таблиця 2.2

Сильні та слабкі сторони про збирання персональних даних різних компаній

Назва компанії	Слабкі сторони	Сильні сторони
Google	Можливість збирання та використання даних для рекламних цілей. Вразливості в програмному забезпеченні та можливість атак на облікові записи користувачів. Проблеми з конфіденційністю деяких особистих даних.	Широкий спектр заходів безпеки, включаючи шифрування даних. Двофакторна аутентифікація для підвищення безпеки облікових записів. Строгі політики конфіденційності та контролю доступу.
Apple	Обмежена можливість настроювання та налаштування для користувачів. Залежність від власної екосистеми та обмежений доступ до додатків сторонніх розробників. Виникнення потенційних вразливостей у нових версіях програмного забезпечення.	Використання шифрування даних на пристроях для зберігання даних в зашифрованому вигляді. Строгі політики конфіденційності та контролю доступу до особистих даних. Захист від атак на пристроях та в хмарних послугах.
Amazon	Велика кількість сервісів та складна конфігурація, що може призводити до налаштування помилок. Вразливості залежностей стороннього програмного забезпечення. Вирішення проблем з безпекою даних на боці користувачів, наприклад, слабкі паролі.	Високі стандарти безпеки в хмарних послугах. Застосування шифрування даних та механізмів контролю доступу. Фізична безпека дата-центрів.
Microsoft	Наявність вразливостей у програмному забезпеченні, що можуть бути використані для атак. Проблеми з конфіденційністю під час певних судових розслідувань або правових вимог. Вплив масштабних кібератак на послуги Microsoft та безпеку користувачів.	Використання шифрування даних та механізмів аутентифікації та авторизації. Політики безпеки, що контролюють доступ до даних та права користувачів. Захист даних у хмарних послугах та на пристроях.

Після огляду таблиці з сильними та слабкими сторонами захисту інформації на прикладі відомих підприємств (Google, Apple, Amazon і Microsoft), можна зробити декілька висновків:

Відомі підприємства докладають значних зусиль для захисту інформації своїх користувачів. Вони використовують широкий спектр заходів безпеки, таких як шифрування даних, двофакторна аутентифікація, строгі політики конфіденційності та контролю доступу.

Серед сильних сторін захисту інформації можна виділити використання шифрування даних, механізмів аутентифікації та авторизації, а також фізичну безпеку дата-центрів. Ці підходи сприяють забезпеченню конфіденційності та цілісності даних.

Серед слабких сторін захисту інформації можна відзначити можливість збирання та використання даних для рекламних цілей, вразливості програмного забезпечення, обмежену можливість настроювання для користувачів, а також потенційні проблеми з безпекою під час судових розслідувань або виконання правових вимог.

Важливо враховувати, що заходи захисту можуть змінюватися з часом. Компанії постійно покращують свої практики та вирішують виявлені проблеми безпеки.

Підприємства повинні продовжувати зосереджувати зусилля на захисті інформації та вдосконалювати свої практики, оскільки безпека особистих даних є надзвичайно важливою для забезпечення довіри користувачів та захисту їх приватності.

2.2. Визначення недоліків та проблем практики захисту особистих даних на підприємствах

Переходимо безпосередньо до створення корпоративної системи захисту персональних даних. Як я вже описав вище, загрози можуть бути різного характеру,

наприклад атаки на програмне забезпечення, спроби несанкціонованого доступу, фізичні загрози, фізичні загрози. Метою нашої системи є прогнозування та запобігання можливим витокам даних. Слід обирати програмне та апаратне забезпечення, яке забезпечує цілісність та конфіденційність інформації.

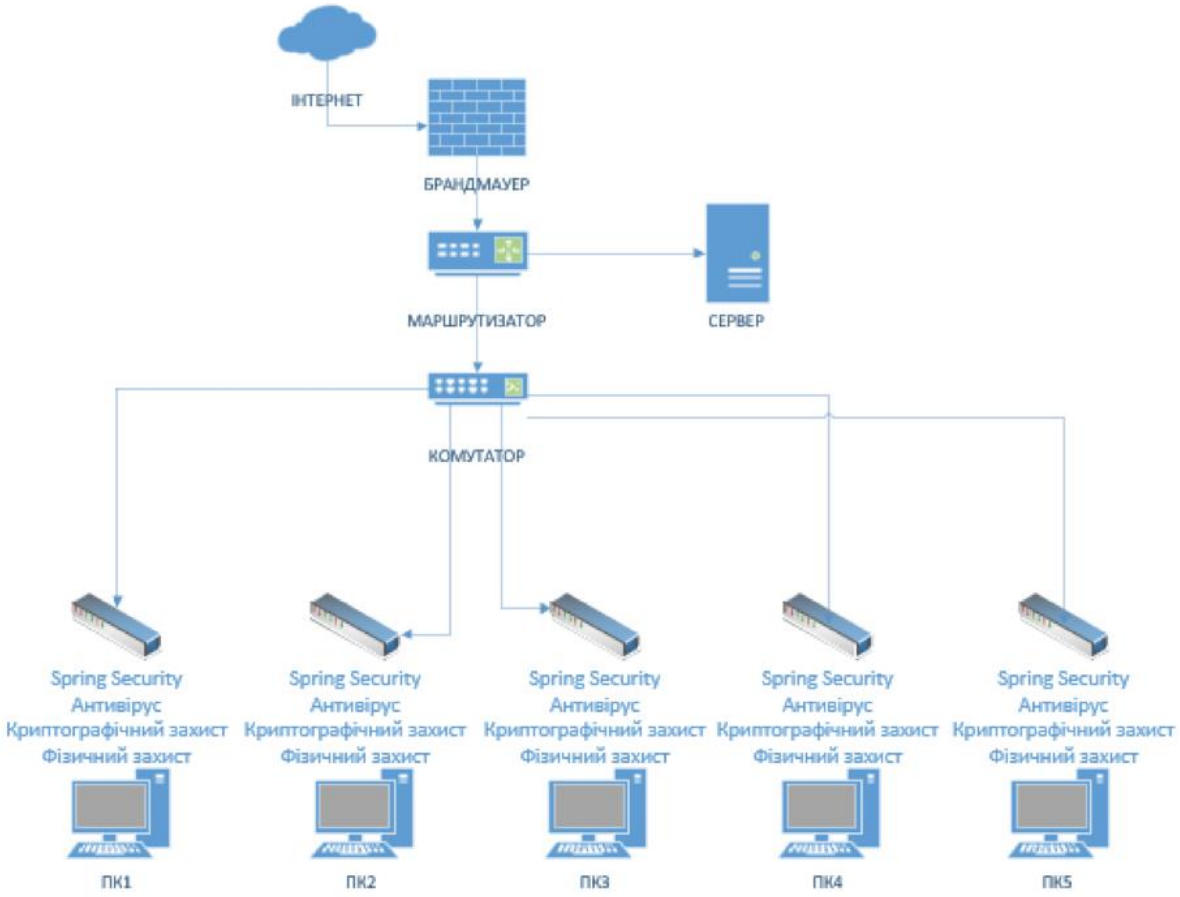

Рисунок 2.4 - Схема системи захисту особистої інформації на підприємстві

По-перше, ви повинні створити систему авторизації/автентифікації, щоб зловмисник не міг просто отримати доступ до даних. Доступ до цієї інформації мають лише відділи, відповідальні за обробку та захист цих даних. Одним із найкращих фреймворків для впровадження авторизації та автентифікації є Spring Security. Це потужна, проста в налаштуванні система автентифікації та контролю доступу. Це стандарт де-факто для захисту додатків на основі Spring. Spring Security — це фреймворк, орієнтований на забезпечення автентифікації та авторизації для програм Java. Як і всі проекти Spring, справжня сила Spring Security полягає в тому, що його

можна легко розширити відповідно до ваших власних вимог. Архітектура фреймворку показана нижче.

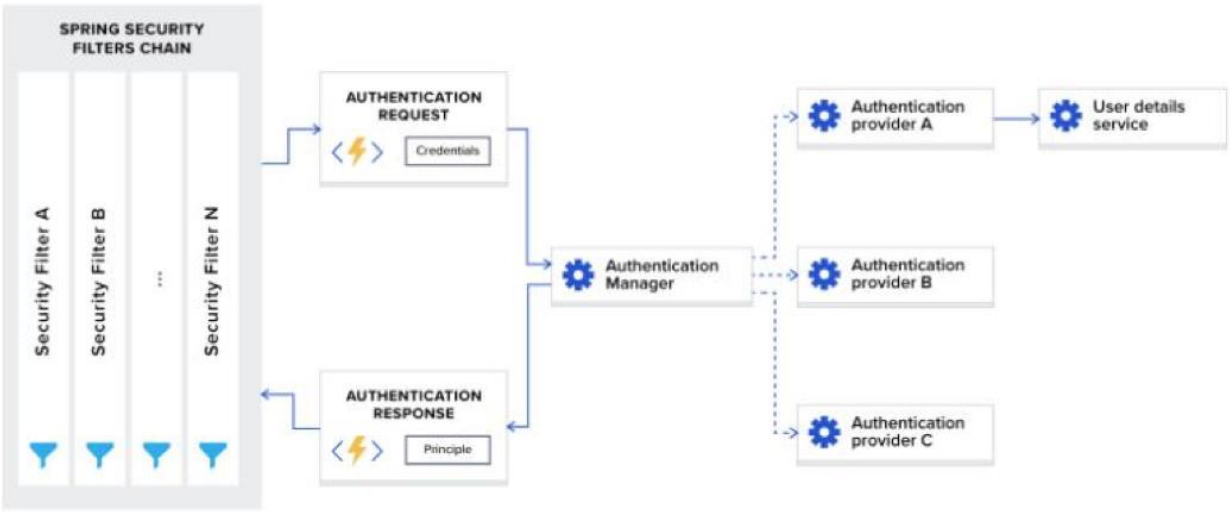

Рисунок 2.5 - Робота Spring Security

Коли ви додаєте структуру безпеки Spring у свою програму, вона автоматично реєструє ланцюжок фільтрів для перехоплення всіх вхідних запитів. Ланцюжок складається з різних фільтрів, кожен з яких обробляє певний варіант використання.

Наприклад: перевірте, чи доступні URL-адреси є загальнодоступними на основі конфігурації. У разі автентифікації на основі сеансу перевіряє, чи користувач уже автентифікований у поточному сеансі. Перевірте, чи має користувач право виконувати запитану дію тощо.

Незважаючи на сильні сторони захисту особистих даних, відомі підприємства (Google, Apple, Amazon і Microsoft) також стикаються з недоліками та проблемами у своїх практиках захисту особистих даних. Ось кілька недоліків та проблем, які відзначели:

1. Збір та використання даних для рекламних цілей: У деяких випадках ці підприємства збирають значну кількість даних про користувачів для персоналізації реклами. Це може порушувати приватність користувачів та створювати ризик неправильного використання цих даних.

2. Вразливості програмного забезпечення: Жодне програмне забезпечення не є повністю вільним від помилок, і це стосується й відомих підприємств. Вразливості програмного забезпечення можуть бути використані зловмисниками для отримання незаконного доступу до особистих даних.

3. Обмежена можливість настроювання для користувачів: В деяких випадках відомі підприємства мають обмежені можливості настроювання для користувачів. Це може обмежувати їх контроль над тим, як їхні дані збираються, використовуються та обробляються.

4. Вимоги правових органів та судових розслідувань: У деяких випадках відомі підприємства можуть знаходитися під тиском правових органів або судових розслідувань, що може впливати на їх здатність забезпечити повну конфіденційність особистих даних користувачів.

5. Вразливості стороннього програмного забезпечення: Відомі підприємства часто використовують стороннє програмне забезпечення, яке може мати свої власні вразливості. Це може створювати ризик для безпеки інформації, якщо ці вразливості використовуються зловмисниками.

6. Масштабні кібератаки: Великі підприємства, такі як Google, Apple, Amazon і Microsoft, стають метою масштабних кібератак через значну кількість даних, які вони зберігають. Такі атаки можуть призвести до несанкціонованого доступу до особистих даних користувачів та порушення їх конфіденційності.

Враховуючи ці недоліки та проблеми, відомі підприємства постійно працюють над вдосконаленням своїх практик захисту особистих даних. Вони інвестують у дослідження та розвиток нових технологій безпеки, співпрацюють з експертами з кібербезпеки та вдосконалюють свої політики та процедури, щоб забезпечити максимальний рівень захисту для своїх користувачів.

РОЗДІЛ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ОСОБИСТИХ ДПНИХ ПРАЦІВНИКІВ НА ПІДПРИЄМСТВІ

3.1. Розробка рекомендацій щодо захисту особистих даних працівників на підприємстві

Організація безпеки даних та інформаційного захисту допомагає відомчим установам, компаніям переглядати політики, впроваджувати ефективні засоби захисту особистих даних клієнтів, партнерів, співробітників. Безпека в цьому випадку базується на таких основних моментах:

- оцінки поточного стану технічної, апаратної складової системи, що використовується, пошуку вразливих місць;

- організації систем захисту персональних даних, реалізованих компаніями, установами (це політики, у тому числі формується загальний регламент);

- відповідності паролів міжнародним стандартам;

- відпрацювання контрдій, впровадження засобів захисту персональних даних в організації, які застосовуються у разі спроби несанкціонованого доступу до інформації.

Організація захисту конфіденційних даних включає роботу з персоналом. Це зумовлено тим, що у 80% випадків саме працівники стають ініціаторами проникнення шкідливих програм у систему. Таке відбувається без злого наміру з боку працівника. Проникають віруси в такий спосіб:

- з оновленнями ПЗ;

- через листи, що надходять на електронну пошту;

- під час переходу за посиланнями;

- через знімні носії інформації.

Організація робіт із захисту персональних даних ґрунтується, в тому числі, і на роботі з персоналом. Складаються інструкції та політики, обов'язкові для ознайомлення, проводяться заняття як реального часу.

Це підвищить безпеку, ефективність протидії спробам несанкціонованого проникнення системи для крадіжки інформації. Кваліфіковані співробітники підрозділу стежать за виконанням політики конфіденційності, запобігають несанкціонованим проникненням у систему третіх осіб.

Організація захисту інформаційної системи персональних даних вимагає комплексного підходу, заснованого на роботі над апаратною, програмною складовою та навчанням персоналу. Тільки так можна створити ефективну протидію віртуальним загрозам, убезпечити інформацію від витоку.

Системи та заходи щодо організації захисту даних

Наше завдання – забезпечити збереження даних, виключити втрату доступу до них відповідальних осіб, запобігти проникненню третіх осіб. Заходи захисту персональних даних в організації включають:

- автоматичного тайм-ауту терміналу користувача Якщо вона не використовується, для повторного відкриття потрібна ідентифікація та пароль;

- автоматичного відключення ідентифікатора користувача під час введення кількох помилкових паролів, файл журналу подій (моніторинг спроб злому);

- системи захисту даних в організації вимагають розробки політики персоналу. У ній визначаються права кожного працівника на доступ до персональних даних;

- інформування персоналу про обов'язки та наслідки за будь-які їх порушення. забезпечення працівникам доступу до персональних даних та ресурсів у рамках виконання службових обов'язків;

- контролю доступу до використання певних областей систем обробки даних.

План заходів щодо захисту персональних даних в організації складається на основі аналізу наявних ресурсів та цілей, які ставить перед фахівцями замовник. Потім він узгоджується із організацією та починається реалізація. Завершальна стадія

– перевірка ефективності, працездатності запроваджених методів, встановленого устаткування.

Системи захисту це не тільки віртуальний, а й фізичний захист. Це означає необхідність обмеження доступу до приміщень, де розміщується серверне обладнання (установка сигналізації, СКУД, обладнання постів охорони).

з використанням інформаційних систем (а значить, і електронних пристроїв), з'являються нові потенційні загрози, які потрібно звести до мінімуму, а краще виключити. Розглянемо їх.

Загрозою інформації вважають можливий вплив або вплив на автоматизовану систему обробки зсередини або ззовні, що спричиняє будь-які негативні наслідки для суб'єктів цієї інформації. Зазвичай інформаційні системи стають особливо вразливими, коли:

- програмне забезпечення компанії недосконале, давно не оновлювалося та містить уразливості;

- деякі процеси системи (зокрема, захисні) функціонують над повну силу;

- ускладнені умови експлуатації та зберігання інформації.

Загрози прийнято поділяти на кілька груп (в основі класифікації лежить природа загрози):

Об'єктивна. Вона безпосередньо залежить від того, наскільки грамотно підібрано обладнання для зберігання та обробки, чи працює належним чином захисне програмне забезпечення.

Типові проблеми:

- несправність технічних засобів,

- слабкі антивіруси, відсутність шлюзів безпеки,

- неможливість зорового контролю над серверами і доступом до них.

Передбачити всі можливі збої та неполадки неможливо, але важливо знати, де і чому вони можуть потенційно статися — і підстрахуватися.

Випадкова. Ця група включає непередбачені обставини, різні НП і системні збої. В даному випадку важливо бути готовими оперативно їх усунути (будь-які

несправності технічних засобів на різних рівнях системи, у тому числі тих, які відповідають за контроль доступу, старіння та знос окремих мікросхем, носіїв даних, лінійних з'єднань, несправність у роботі антивірусних, сервісних та прикладних. програм).

Суб'єктивна. Як правило, під такими загрозами розуміють неправильні дії працівників, які здійснюють технічну обробку, зберігання та захист інформації. Вони можуть помилятися у дотриманні правил безпеки та допускати витоку при завантаженні програмного забезпечення або в момент активного використання системи, при різних маніпуляціях з базами даних, при включенні та вимкненні апаратури. Також до цієї групи належать неправомірні дії колишніх співробітників, які залишили несанкціонований доступ до даних.

Фахівці компанії-оператора мають враховувати всі типи загроз. До уваги слід взяти критерії, які допоможуть зрозуміти, якою є реальна можливість загрози того чи іншого типу (а також ймовірність поломки або успішного обходу захисних алгоритмів):

Доступність. Цей критерій демонструє, наскільки просто зловмисник може отримати доступ до потрібної інформації або до інфраструктури організації, де зберігаються ці дані.

Фатальність. Ця характеристика передбачає оцінку ступеня глибини впливу загрози загальне функціонування системи та здатність спеціального персоналу підприємства впоратися з наслідками впливу цього чинника.

Кількість. Це параметр, що передбачає визначення кількості потенційно вразливих деталей системи зберігання та обробки даних.

Точний розрахунок ймовірності впливу тієї чи іншої загрози виробляється математично – це можуть зробити аналітичні експерти компанії. Такий самоаналіз дозволяє об'єктивно оцінити ризики та вжити додаткових заходів захисту: закупити досконаліше обладнання, провести додаткове навчання працівників, перерозподілити права доступу тощо.

Існує кілька інших, більш докладних класифікацій внутрішніх та зовнішніх загроз, які будуть корисними для систематизації всіх факторів.

Навмисність втручання:

- загроза, спричинена недбалістю співробітників, які працюють з інформаційною системою;

- загроза, що ініціюється суб'єктами ззовні з метою отримання особистої вигоди.

Характеристики появи:

- Штучна загроза, створена за участю людини;

- природна, непідконтрольна людині (найчастіше - стихійні лиха).

Безпосередня причина загрози:

- Людина, що розголошує суворо конфіденційні відомості;

природний чинник (незалежно від масштабу);

- спеціалізоване шкідливе програмне забезпечення,

- Порушує роботу системи;

- видалення даних випадковим шляхом через відмову техніки.

Момент впливу загрози на інформаційні ресурси:

- у момент обробки інформації (зазвичай це відбувається через розсилки вірусних утиліт);

- При отриманні системою нової інформації;

- незалежно від ступеня активності роботи системи (наприклад, при спрямованому зламі шифрів або криптозахисту).

Існують і інші класифікації, що враховують серед параметрів можливість доступу працівників до самої системи або її елементів, спосіб доступу до основних частин системи та конкретні способи розміщення інформації.

Значну частину всіх загроз експерти пов'язують із об'єктивними зовнішніми чинниками та інформаційним вторгненням з боку конкурентів, зловмисників та колишніх співробітників. Особливу небезпеку становлять ті з них, хто знайомий з

правилами функціонування конкретної системи, має знання на рівні розробника програм і має відомості про те чи інше вразливе місце в системі.

Інформаційна безпека передбачає чотири рівні захисту від загроз:

Перший рівень. Найбільш високий, передбачає повний захист спеціальних персональних даних (національна та расова приналежність, ставлення до релігії, стан здоров'я та особисте життя).

Другий рівень. Передбачає захист біометричних даних (зокрема фотографії, відбитки пальців).

Третій рівень. Це захист загальнодоступних даних, тобто тих, до яких повний і необмежений доступ надано самою людиною.

Четвертий рівень. Це збірна група, куди включають усі дані, не згадані у попередніх трьох пунктах.

Таким чином, усі дані, зібрані в інформаційній базі компанії, можуть бути чітко розподілені за рівнем захисту.

Забезпечення захисту

Захист інформації за рівнями у кожному випадку складається з ланцюжка заходів.

Четвертий рівень. Означає виняток із приміщення, де знаходиться інформаційне обладнання, сторонніх осіб, забезпечення збереження носіїв даних, затвердження чіткого списку працівників, які мають допуск до обробки даних, а також використання спеціальних засобів захисту інформації.

Третій рівень. Має на увазі виконання всіх вимог, передбачених для попереднього рівня, та призначення відповідальної за інформаційну безпеку посадової особи.

Другий рівень. Крім виконання вимог попереднього рівня, включає обмеження доступу до електронного журналу безпеки.

Перший рівень. Окрім усіх вимог, яким необхідно дотримуватися другого рівня, включає забезпечення автоматичної реєстрації в електронному журналі безпеки повноважень працівників, які мають доступ до даних, у разі зміни цих

повноважень, а також покладання відповідальності за інформаційну безпеку на спеціально створений підрозділ.

Належне виконання прописаних у законодавстві заходів захисту персональних даних відповідно до рівня забезпечує максимальну ефективність загальної стратегії захисту інформації, прийнятої в компанії-операторі.

Одним із найбільш дієвих способів захисту персональних даних є використання засобів криптографії.

До криптографічних засобів належать апаратні, програмні та комбіновані пристрої та комплекси, здатні реалізовувати алгоритми криптографічного перетворення інформації.

Вони призначені одночасно для захисту інформації при передачі каналами зв'язку та захисту її від недозволеного доступу при обробці та зберіганні. Логіка проста: зловмисник, який не знає коду, не зможе скористатися даними, навіть якщо отримає доступ до них, оскільки не прочитає їх. Для нього вони залишаться безглуздим набором начебто випадкових цифр.

Обробка ПД є дії з ПД, включаючи збір, систематизацію, накопичення, зберігання, уточнення (оновлення, зміна), використання, поширення (у тому числі передачу), знеособлення, блокування, знищення.

Зберігання ПД повинно здійснюватися у формі, що дозволяє визначити суб'єкта персональних даних, не довше, ніж цього вимагають мети їх обробки, і вони підлягають знищенню після досягнення цілей обробки або у разі втрати потреби у їх досягненні.

Таблиця 3.1

Основні засади обробки персональних даних

№п/п	**Назва принципу**	**Пояснення**
1.	Законність цілей та способів	Законність цілей та способів обробки персональних даних та сумлінності
2.	Відповідність цілей обробки заздалегідь визначеним цілям	Відповідність цілей обробки персональних даних цілям, заздалегідь визначеним та заявленим при

		зборі персональних даних, а також повноваженням оператора
3.	Відповідність способів обробки цілям обробки	Відповідність обсягу і характеру оброблюваних персональних даних, способів обробки персональних даних цілям обробки персональних даних

продовження табл. 3.1

4.	Достовірність, достатність даних	Достовірність персональних даних, їх достатність для цілей обробки, неприпустимість обробки персональних даних, надлишкових по відношенню до цілей, заявлених під час збору персональних даних
5.	Неприпустимість об'єднання баз даних ІС	Неприпустимість об'єднання створених для несумісних між собою цілей баз даних інформаційних систем персональних даних

Під технічними засобами, що дозволяють здійснювати обробку ПД, розуміються засоби обчислювальної техніки, інформаційно-обчислювальні комплекси та мережі, засоби та системи передачі, прийому та обробки ПД (засоби та системи звукозапису, звукопідсилення, звуковідтворення, переговорні та телевізійні пристрої, засоби виготовлення, тиражування документів та інші технічні засоби обробки мовної, графічної, відео та буквено-цифрової інформації), програмні засоби (операційні системи, системи управління базами даних тощо), засоби захисту інформації, що застосовуються в інформаційних системах.

Безпека ПД досягається шляхом виключення несанкціонованого, у тому числі випадкового, доступу до персональних даних, результатом якого може стати знищення, зміна, блокування, копіювання, розповсюдження ПД та інших несанкціонованих дій. Безпека ПД під час їхньої обробки в інформаційних системах забезпечується за допомогою системи захисту ПД.

Засоби захисту інформації, які застосовуються в інформаційних системах, в установленому порядку проходять процедуру оцінки відповідності. Для розроблення та здійснення заходів щодо забезпечення безпеки ПД під час їх обробки в ІС

оператором або уповноваженою особою може призначатися структурний підрозділ або посадова особа (працівник), відповідальні за забезпечення безпеки ПД. Для захисту інформації, що передається каналами зв'язку, існує чотири основних класи методів захисту:

1) фізичні;

2) апаратні;

3) програмні;

4) організаційні.

На рис. 3.1 показано чотири рівні захисту, розташовані в тій послідовності, в якій вони захищають інформацію, що зберігається на комп'ютері.

Організаційний захист характеризується сукупністю організаційно-технічних заходів, розробкою та прийняттям законодавчих актів з питань захисту інформації тощо.

Фізичний захист використовується на верхніх рівнях захисту і полягає у фізичному запобіганні доступу сторонніх осіб до процесу обробки даних. Для фізичного захисту застосовуються засоби: служба охорони, що складається з кваліфікованих працівників служб безпеки; лазерні та оптичні системи, що реагують на перетин порушником світлових променів; системи нейтралізації випромінювань; системи захисту вікон та дверей від несанкціонованого проникнення тощо.

Апаратний захист реалізується апаратурою у складі ЕОМ або за допомогою спеціалізованих пристроїв. До апаратних засобів захисту належать різні схеми блокування від несанкціонованого використання.

Програмний захист реалізується за допомогою різноманітних програм: операційних систем; програм обслуговування; антивірусних пакетів; інструментальних; спеціалізованих програм захисту; прикладних програм.

Рисунок 3.1 - Рівні захисту в системі передачі даних

Рисунок 3.2 - Діаграма нульового рівня захисту персональних даних

За допомогою програмно-апаратних засобів можна вирішувати як основні завдання інформаційно-програмного забезпечення (від розкрадання, від втрати, від збоїв та відмов обладнання), так і захист від помилок у програмах.

Розв'язання цих завдань забезпечується такими способами:

1. Захист від несанкціонованого доступу до ресурсів з боку користувачів та програм.

2. Захист від несанкціонованого використання ресурсів за наявності доступу.

3. Захист від некоректного використання ресурсів.

4. Внесенням структурної функціональної та інформаційної надмірності.

5. Висока якість розробки програмно-апаратних засобів.

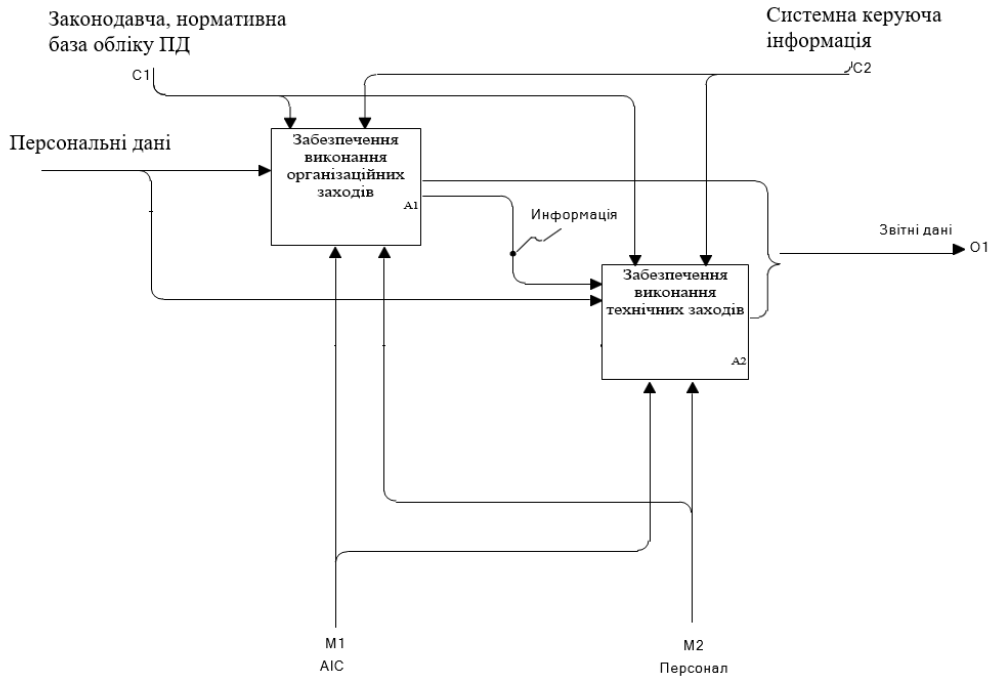

Рисунок 3.3 - Діаграма першого рівня "Захист персональних даних"

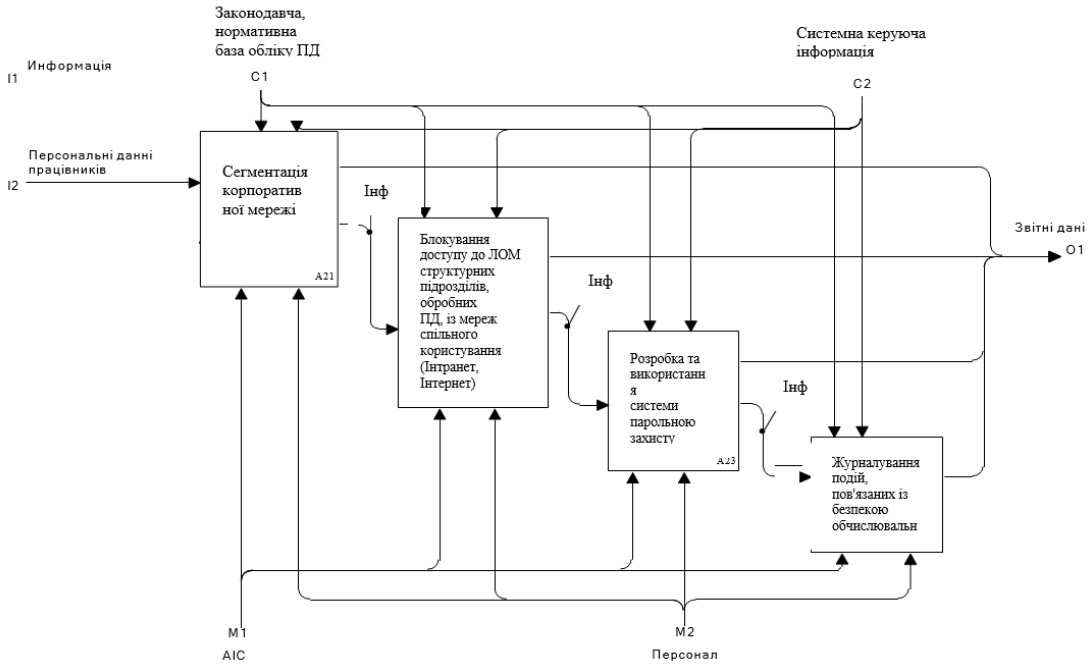

Рисунок 3.4 - Діаграма другого рівня "Забезпечення виконання технічних заходів"

На рисунках 3.2.-3.6. представлений комплекс взаємозалежних діаграм, розроблених "згори-вниз" методом декомпозиції, що дозволяє відобразити сукупність заходів, методів та засобів захисту персональних даних в підприємстві. Аналіз спроектованих діаграм дозволив сформувати план дій із захисту ПД на підприємстві.

Загальний перелік технічних заходів щодо захисту ПД на підприємстві включає:

- запобігання несанкціонованому доступу до ПД (регламентування доступу працівників до обробки ПД, парольний та антивірусний захист);
- проведення заходів, спрямованих на своєчасне виявлення фактів несанкціонованого доступу до ПД (регламентування використання та регулярне оновлення антивірусних засобів);
- недопущення впливу на технічні засоби автоматизованої обробки ПД, внаслідок якого може бути порушено їхнє функціонування (охорона та регламентування використання технічних засобів);
- можливість негайного відновлення ПД, модифікованих чи знищених внаслідок несанкціонованого доступу до них (зберігання резервних копій на знімних маркованих носіях).

Рисунок 3.5 - Перелік розроблених рекомендацій щодо забезпечення захисту персональних даних

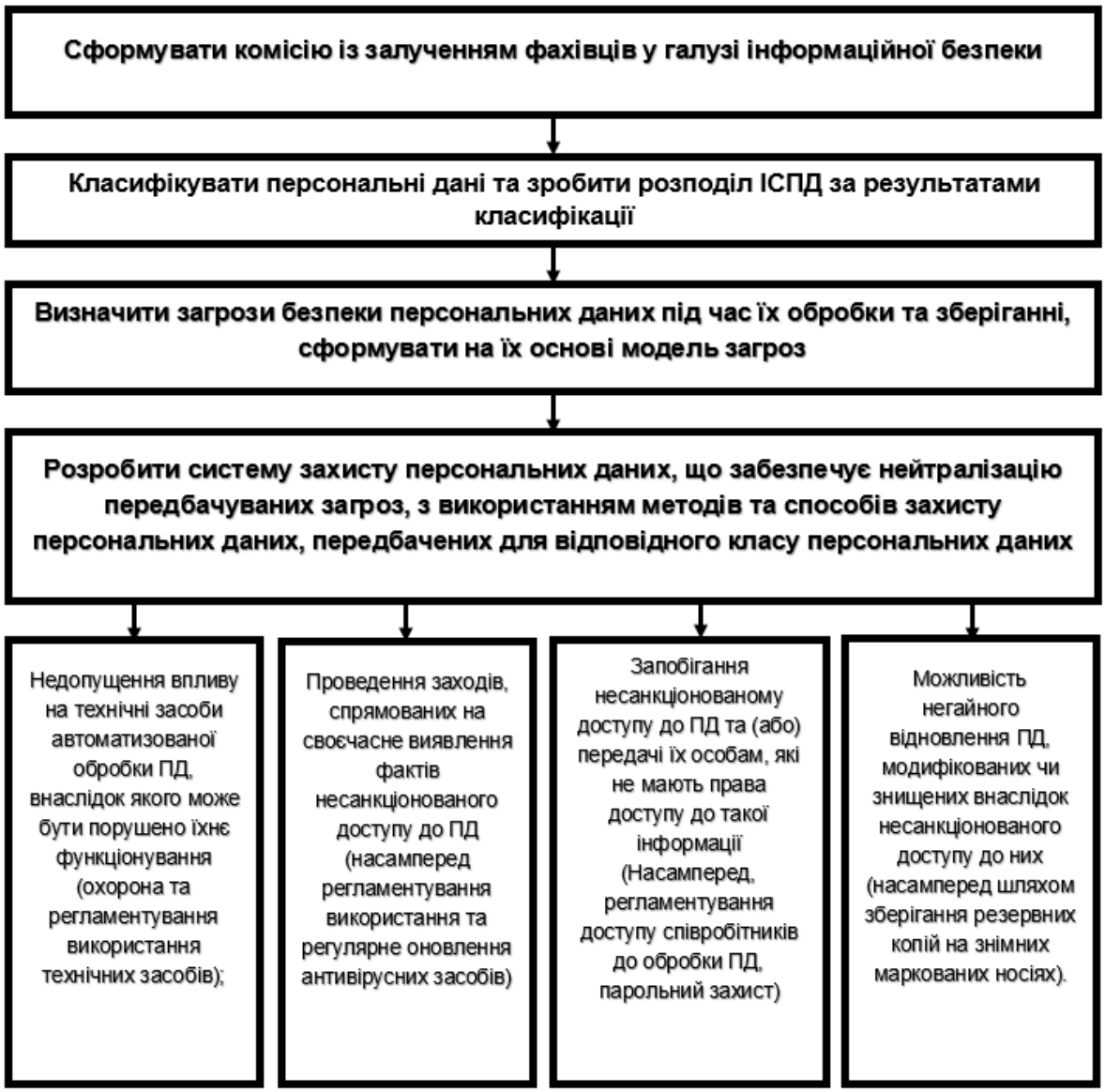

Рисунок 3.6 - Перелік розроблених рекомендацій щодо технічного захисту персональних даних

Як бачимо, підтримка системи інформаційної безпеки є досить трудомістким завданням. Не кожен бізнес чи державна компанія можуть дозволити собі штат профільних фахівців. У багатьох випадках простіше віддати це завдання на аутсорс, найняти сторонніх фахівців, які допоможуть підібрати та встановити відповідне обладнання, проконсультую персонал, підтримають написання політики конфіденційності та внутрішніх регламентів щодо поводження із засекреченою інформацією.

Така співпраця завжди вимагає великого залучення з боку керівної ланки компанії та всіх її співробітників. Неуважність та недостатньо серйозне ставлення до дотримання заходів захисту можуть закінчитися крадіжкою даних, великими штрафами, судовими розглядами та репутаційними втратами.

Регулярно проводьте оцінку ефективності обраних заходів захисту, оперативно вносите корективи, слідкуйте за змінами законодавства. Попередити загрозу в рази простіше (і дешевше), ніж боротися із її наслідками.

3.2. Оцінка ефективності розроблених методів та стратегій

Захист особистих даних працівників на підприємстві є надзвичайно важливим завданням в епоху цифрових технологій та зростаючих загроз безпеці. У цій оцінці ми проведемо аналіз розроблених методів та стратегій захисту, використовуючи дані з попередніх повідомлень, та визначимо їх ефективність.

1. Класифікація та ідентифікація даних:

- Оцінка ефективності методів класифікації особистих даних та механізмів контролю доступу.

- Визначення рівня конфіденційності та його впливу на ефективність захисту.

2. Забезпечення безпеки даних:

- Оцінка вибору методу шифрування та його відповідності вимогам безпеки.

- Аналіз застосування симетричного шифрування, асиметричного шифрування та хеш-функцій.

3. Захист від втрати даних:

- Оцінка стратегії резервного копіювання та її ефективності в уникненні втрати даних.

- Аналіз процедур відновлення даних та їх впливу на час відновлення та безпеку.

4. Міцний пароль та аутентифікація:

- Оцінка міцності паролів та їх впливу на безпеку особистих даних.

- Аналіз ефективності багатофакторної аутентифікації та її впровадження на підприємстві.

5. Навчання та свідомість працівників:

- Оцінка ефективності навчальних семінарів та програми навчання працівників.

- Вимірювання рівня свідомості працівників щодо політики безпеки та практик безпеки.

6. Моніторинг та аудит:

- Оцінка систем моніторингу та аудиту щодо їх здатності виявляти потенційні загрози.

- Аналіз результатів аудиту безпеки та їх впливу на удосконалення стратегій захисту.

Залежно від результатів оцінки ефективності кожного методу та стратегії, можна зробити висновки щодо їх відповідності потребам безпеки особистих даних працівників на підприємстві. Необхідно звернути увагу на сильні та слабкі сторони кожного методу та стратегії і розробити план подальших дій для їх удосконалення та оптимізації.

Ця оцінка надасть підстави для прийняття рішень щодо подальшого розвитку та вдосконалення системи захисту особистих даних працівників на підприємстві та забезпечить ефективний захист цінних інформаційних активів.

У результаті проведеного аналізу було визначено такі недоліки: - відсутній засіб реалізації представлених методів оцінки ефективності; – алгоритмічна складність застосування запропонованих методів; – не розглянуто метод підтримки прийняття рішень у системах захисту персональних даних на основі експертного підходу. Метою роботи є усунення перелічених вище недоліків, за допомогою визначення оптимального методу при проведенні оцінки ефективності заходів щодо забезпечення безпеки ПД у працівників на підприємстві. Для досягнення поставленої мети вирішені наступні завдання: - Проведено порівняльний аналіз методів підтримки прийняття рішень у задачі системи захисту ПД; – побудовано ієрархічну структуру завдання

оцінки ефективності у працівників на підприємстві; - Проведено автоматизований розрахунок оцінки ефективності захисних заходів на основі методу аналізу ієрархій. Робота з підготовки прийняття рішень часто є занадто трудомісткою для однієї людини. Несвоєчасно прийняте рішення може негативно позначитися на всіх системах захисту персональних даних і призвести до витоків та матеріальних збитків. Важливим завданням освітньої організації є вибір найефективнішого методу, застосовуваного для систем захисту персональних даних.

Система захисту персональних даних у працівників на підприємстві модифікується у процесі експлуатації, що потребує застосування методу, здатного підтримувати змінність системи та враховувати багатокритеріальність вибору. Проведений порівняльний аналіз методів підтримки прийняття рішень показав, що метод аналізу ієрархій можна застосувати для вирішення завдань захисту персональних даних. Особливістю методу аналізу ієрархій є його універсальність, яка враховує багатокритеріальність вибору в умовах невизначеності, та відповідає вимогам простоти підготовки та обробки експертної інформації. Метод аналізу ієрархії є систематичною процедурою для ієрархічного представлення елементів. Суть методу полягає в декомпозиції завдання на простіші складові частини та подальшої обробки послідовних суджень аналітика з парних порівнянь. Алгоритм застосування методу аналізу ієрархій складається з кількох етапів:

1) структурування проблеми вибору як ієрархії;

2) встановлення пріоритетів критеріїв та оцінка кожної з альтернатив за критеріями;

3) визначення коефіцієнтів важливості елементів кожного рівня; 4

4) підрахунок комбінованого вагового коефіцієнта та визначення найкращої альтернативи.

Приступаючи до оцінки ефективності заходів захисту з допомогою застосування методу аналізу ієрархій, необхідно розробити систему критеріїв, якими виконуватиметься аналіз. Ефективність кожного заходу захисту інформації оцінюється локальними показниками ефективності. Їх можна поділити на

функціональні та економічні. Функціональні показники характеризують рівень безпеки інформації, економічні – Витрати її забезпечення. Виходячи з цього твердження пропонуються такі показники для аналізу та оцінки ефективності: коефіцієнт компенсації ризику, що характеризує відносний ефект від реалізації захисних заходів; коефіцієнт економічної ефективності захисних заходів; показник повернення від інвестицій, що характеризує віддачу від зроблених інвестицій за певний період; показник витратоємності активів; час безпечного функціонування системи. Ієрархічна модель оцінки ефективності заходів захисту може бути представлена таким чином: на найвищому рівні знаходиться глобальна мета – оцінка ефективності реалізованих у рамках захисту персональних даних заходів щодо забезпечення безпеки ПД; продовжується до перерахованих вище критеріїв; далі до альтернатив – висока, середня та низька ефективність.

Проаналізувавши принципи роботи даних програмних забезпечень, виявлено такі недоліки: відсутність можливостей зберігання вихідної інформації для багаторазового використання та порівняння кількох експертних думок; складний інтерфейс користувача; відсутність візуальної наочності.

До переваг застосування методу аналізу ієрархій при оцінці ефективності заходів захисту у працівників на підприємстві можна віднести: - метод аналізу ієрархій має чітке математичне обґрунтування та простоту обчислювальних алгоритмів; - метод здатний підтримувати змінність системи захисту персональних даних та враховувати багатокритеріальність вибору; - метод може бути реалізований у Microsoft Excel. На даний момент проведений розрахунок оцінки ефективності захисних заходів має низку припущень, наприклад, кількість експертів та критеріїв заздалегідь прописана. Для зміни матриці судження потрібно редагування формул у багатьох осередках. Тим не менш, даний підхід простий у розумінні та реалізації.

Проведений порівняльний аналіз методів підтримки прийняття рішень показав, що найбільш оптимальним є метод аналізу ієрархій, який може бути застосований у завданнях захисту персональних даних. Побудовано ієрархічну структуру завдання оцінки ефективності у навчальному закладі. Проведено автоматизований розрахунок

оцінки ефективності захисних заходів у системах захисту персональних даних на основі методу аналізу ієрархій. Застосування методу аналізу ієрархії щодо оцінки ефективності заходів захисту дозволяє наочно показати визначення підсумкової оцінки з урахуванням обраних альтернатив.

Перевірка інформаційної системи персональних даних здійснюється в обов'язковому та добровільному порядку та дозволяє визначити, наскільки продуктивно вона функціонує, точніше — чи справляються передбачені заходи захисту зі своїми завданнями, а саме:

- чи є всі передбачені чинним законодавством елементи, наскільки коректно вони налаштовані та інстальовані;

- чи є повний перелік документів захисту особистої інформації, чи відповідає він чинним правовим нормативам;

- чи призначені відповідальні особи за забезпечення безпеки ПД, наскільки вони компетентні та справляються з поставленими завданнями;

- чи обізнані користувачі системи у сфері захисту персональних даних;

Для складання остаточного вердикту фахівцям необхідно проаналізувати відповідність організаційно-технічним вимогам та випробовувати впроваджені захисні заходи від потенційних загроз. За підсумками кожного тесту та етапу заповнюються протоколи, а висновки відображаються у підсумковому висновку.

Перед початком робіт співробітники Центру розробляють методику, в якій описується порядок досліджень, опис об'єкта, список запланованих процедур, критерії та вимоги, якими керуватимуться.

Безпосередньо оцінка ефективності захисту персональних даних включає аналіз:

- структурні особливості системи;

- технологічних аспектів обробки персональних даних суб'єктів;

- достатності внутрішньої документації, її відповідності прописаним у нормативно-правових актах вимогам;

- відповідності між структурою, складом програмно-технічної бази ІСПД та підготовленою організаційно-технічною документацією;

- правильності визначення рівнів захищеності персональних даних та способів захисту для кожного з них;

- підготовленості персоналу та розподілу відповідальності;

- наявності та результативності фізичної охорони ІСПД;

- стану та виконання робіт з підтримки безпеки інформаційної системи.

Щоб переконатися в тому, що ІСПД надійно захищена від несанкціонованого проникнення, витоку даних та інших загроз, наші співробітники проводять за допомогою спеціального обладнання та програмного забезпечення випробування всіх підсистем:

- обліку та реєстрації;

- контролю доступу;

- антивірусного захисту;

- підтримки цілісності;

- міжмережевого екранування;

- виявлення вторгнень;

- каналів зв'язку;

- оцінки безпеки.

Оціночні роботи включають визначення наявності передбаченої законом документації (проектної, експлуатаційної), її відповідності комплексу програмно-технічних засобів і ступеня виконання правил використання СЗІ.

Розроблені етапи оцінки методів захисту ПД

1. Оцінка документації, пов'язаної з ПД

1.1 Перевірка цілей обробки ПД

1.2 Перевірка законності обробки персональних даних

1.3 Перевірка термінів обробки ПД

2. Оцінка політики інформаційної безпеки

2.1 Обґрунтованість вибору типу порушника

2.2 Актуальність певних загроз

2.3 Відповідність заходів щодо захисту

2.4 Обґрунтованість вибору складу та класів технічних засобів захисту

2.5 Наявність переліку інформаційних ресурсів, що захищаються, і матриця доступу до інформаційних ресурсів

2.6 Наявність інструкцій та призначення відповідального за організацію процесу забезпечення захисту

2.7 Наявність нормативної та необхідної організаційно-розпорядчої документації

3. Оцінка класифікації та рівня захищеності ІСПД

3.1 Наявність документа, що відображає інформацію про класифікацію

3.2 Правильність проведеної класифікації

3.3 Оцінка відповідності наявних технічних засобів та засобів захисту інформації, поданим у документації

3.4 Оцінка обраного для інформаційної системи типу актуальних загроз

4. Оцінка документації на технічні засоби захисту

4.1 Наявність паспорта (формуляра) технічного засобу

4.2 Відповідність класу захищеності

5. Оцінка вимог до приміщень, де обробляються ПД

5.1 Перевірка режиму доступу до приміщень

5.2 Захист від зчитування

6. Оцінка відповідності кваліфікації співробітників, які забезпечують захист ПД

6.1 Перевірка знань інструкцій

6.2 Перевірка документів

6.3 Перевірка знання технологій

7. Оцінка аналізу інформаційних потоків

7.1 Зміст інформаційного потоку

7.2 Співвіднесення інформаційних потоків із зовнішніми інформаційними системами та організаціями

7.3 Законна основа передачі персональних даних

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.96 р. No 254/96 // Відомості Верховної Ради України (ВВР). – 1996. – No 30. – Ст. 141.

2. Про інформацію : Закон України від 02.10.1992 р. №2849-IX: станом на 13.12.2022. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

3. Про захист персональних даних : Закон України від 01.06.10 р. No 2297-VI // Відомості Верховної Ради України (ВВР). – 2010. – No 34. – Ст. 481.

4. Брижко В.М. Організаційно-правові питання захисту персональних даних : дис. на здобуття наук. ступеня канд. юрид. наук : спеціальність 12.00.07 / В.М. Брижко. – (НДЦ правової інформатики НАПрН України, Національна академія державної податкової служби). – К., 2004. – 251 с. – С. 168.

5. Виноградова Г.В. Правове регулювання інформаційних відносин в Україні / Г.В. Виноградова . – К, 2006. – 176 с.

6. Брель О. Персональні дані як об’єкт інформаційних правовідносин за участю суб’єктів господарювання // Право України.– 2011. – No 4. – С.220-224.

7. Саєнко М.І. Сучасне правове регулювання інформаційних відносин у сфері захисту персональних даних в Україні // Право і суспільство – 2015. – No 3. – С. 103.

8. Селіванова О.О. Сучасна лінгвістика : термінологічна енциклопедія. – Полтава : Довкілля, 2006.– 716 с.

9. Про захист осіб у зв’язку з автоматичною обробкою персональних даних : Конвенція Ради Європи від 28 січня 1981 року No 108 // Офіційний вісник України.– 2011 – No 1. – С. 701.

10. Про захист фізичних осіб у зв’язку з автоматичною обробкою персональних даних і про вільне переміщення таких даних : Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_242

11. Communication from the Commissions to the European Parliament, the Council the Economic and Social Committee and the Committee of the regions “A comprehensive approach on personal data protection in the European Union”. [Електронний ресурс]. – Режим доступу: http//ec.europa.eu/health/data_ collection/docs/com_2010_0609_en.pdf

12. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частини першої, другої статті 32, частин другої, третьої статті 34 Конституції України No 2-рп/2012. [Електронний ресурс]. – Режим доступу: http://www.ccu.gov.ua/uk/doccatalog/list?currDir=167724

13. Гуцалюк, М. Інформаційна безпека України: нові загрози та організація протидії [Текст] / М. Гуцалюк // Правова інформатика. — 2004. — No 3. — С. 37–41.

14. Г.М. Гулак, В.А. Козачок, П.М. Складанний, М.О. Бондаренко, Б.В. Вовкотруб // Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах. – 2017. – No2(30). – С. 65-70.

15. Німченко, Т. В. Критерій визначення з переліку даних тих, що відносяться до категорії персональні [Текст] / Т. В. Нім ченко // Вісник інженерної академії України. — 2015. — No 1. —С. 199–202.

16. Німченко, Т. В. Алгоритм виявлення несанкціонованого витоку персональних даних мережевими каналами [Текст] / Т. В. Німченко, І. М. Мужик, А. І. Мужик // Вісник інженрної академії України. — 2014. — No 3–4. — С. 199–203.

17. Захист персональних даних на підприємстві / В. Мачуський – 2018. [Електронний ресурс]. – Режим доступу: https://www.businesslaw.org.ua/zahyst-personalnyx-danyx-na-pidpryemstvi/

18. Оніщенко О.В. Конституційне та адміністративне право / Оніщенко О.В. // Захист персональних даних. – 2012 – No1 – С. 60-63.

19. Тунік А. Захист персональних даних: аналіз вітчизняного законодавства / А. Тунік // Право України. – 2011. – No8. – С. 97–100.

20. Щербатюк М. Особливості захисту персональних даних в Інтернеті [Електронний ресурс]. – Режим доступу: https://inau.ua/document/osoblyvosti-zahystu-personalnyh-danyh-v-interneti.

21. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). // Official Journal of the European Union. – 2016.

22. Технічний комітет зі стандартизації «Інформаційні технології» (ТК 20). ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT) // ДП «УкрНДНЦ». – 2018.

23. Documentation for the Cookie Consent plugin [Електронний ресурс]. – Режим доступу: [https://cookieconsent.osano.com/documentation/about-cookie-consent/.

24. Technical Guide to Information Security Testing and Assessment / K.Scarfone, M. Souppaya, A. Cody, A. Orebaugh. // Recommendations of the National Institute of Standards and Technology.

25. Vulnerability & Exploit Database [Електронний ресурс]. – Режим доступу: https://www.rapid7.com/db/.

26. CVE details [Електронний ресурс]. – Режим доступу: https://www.cvedetails.com.

27. Про захист персональних даних : Закон України від 23.02.2012 р. №2297-VI: станом на 27 жовт. 2022р. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text