Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Жевтіла Юрія Юрійовича*

академічної групи *125-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Побудова моделі захисту персональних даних на підприємстві ТОВ «ПФСОФТ»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	к.т.н., доц. Герасіна О.В.			
економічний	к.е.н., доц. Пілова Д.П.	90	відмінно	
Рецензент				
Нормоконтролер				

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Жевтілу Юрію Юрійовичу*** **академічної групи** ***125-19-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Побудова моделі захисту персональних даних на підприємстві ТОВ «ПФСОФТ»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Розбір поняття персональних даних, аналіз існуючих загроз для безпезпеки персональних даних. Формулювання задачі для системи захисту.	25.02.2023 – 31.03.2023
Розділ 2	Побудова системи захисту персональних даних для підприємства ТОВ «ПФСОФТ» з використанням апаратного, програмного та організаційного забезпечення.	01.04.2022 – 12.05.2023
Розділ 3	Розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.	13.05.2022 – 09.06.2023

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Жевтіло Ю.Ю..
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 106 с., 5 рис., 7 табл., 5 додатків, 22 джерела.

Об'єкт розробки – процес захисту персональних даних на підприємстві ТОВ «ПФСОФТ».

Предмет розробки – система захисту персональних даних на підприємстві ТОВ «ПФСОФТ».

Мета кваліфікаційної роботи – створення моделі системи захисту персональних даних на прикладі конкретного підприємства.

Наукова новизна результатів полягає у систематизації існуючих методів захисту персональних даних на прикладі конкретного підприємства, що дозволить у подальшому створювати ефективні та різносторонні системи захисту інформації на інших підприємством з використанням методів, вказаних у роботі.

У першому розділі проаналізований правовий супровід захисту персональних даних, розглянуте саме поняття персональних даних та можливі загрози щодо безпеки персональних даних як на конкретному підприємстві, так і у загальному випадку.

У спеціальній частині роботи розглянуто та класифіковано існуючи методи захисту персональних даних за їх різновидами: апаратні, програмні та організаційні. Побудовано систему захисту персональних даних для підприємства ТОВ «ПФСОФТ». За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.

ПЕРСОНАЛЬНІ ДАНІ, СИСТЕМА ЗАХИСТУ, ІНФОРМАЦІЯ, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ, ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ, ІНФОРМАЦІЙНА СИСТЕМА

ABSTRACT

Explanatory note: p. 111, fig. 4, tab. 7, 5 additions, 22 sources.

The object of development is the personal data protection process at LTD "PFSOFT".

The subject of the development is a system for the collection of personal data at the enterprise of LTD "PFSOFT".

The purpose of the qualification work is to create a model of the personal data protection system based on the example of a specific enterprise.

The scientific novelty of the results consists in the systematization of existing methods of personal data protection on the example of a specific enterprise, which will allow in the future to create effective and versatile information protection systems for other enterprises using the methods specified in the work.

In the first section, the legal support for the protection of personal data is analyzed, the very concept of personal data and possible threats to the security of personal data both at a specific enterprise and in the general case are considered.

In a special part of the work, the existing methods of personal data protection are considered and classified according to their types: hardware, software, and organizational. A personal data protection system was built for the enterprise LTD "PFSOFT". Based on the results of the research, conclusions were made regarding the solution to the problem.

In the economic section, calculations of capital costs, economic effect and payback period of capital investments of the proposed solutions are made.

PERSONAL DATA, PROTECTION SYSTEM, INFORMATION, LONG-TERM SOFTWARE, INFORMATION , HARDWARE, ORGANIZATIONAL SUPPORT

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ЗБПД – загроза безпеки персональних даних;

ЗІ – захист інформації;

ІС – інформаційна система;

ІСПД – інформаційна система персональних даних;

НСД – несанкціонована спроба доступу;

ОЗІБ – організаційне забезпечення інформаційної безпеки;

ОЗП – оперативний запам’ятовуючий пристрій;

ОС – операційна система;

ПД – персональні дані;

ПЕОМ – персональна електронна обчислювальна машина;

ПЗП – постійний запам’ятовуючий пристрій;

СЗ – система захисту;

СЗПД – система захисту персональних даних;

СФЗ – система фізичного захисту;

ЦСК – централізована система керування;

ЗМІСТ

ВСТУП

Актуальність теми.

Одним з найбільш проблемних питань в епоху інформаційних технологій є захист персональних даних. І ці питання виникають, як в межах однієї країни, так і за її межами. Дані користувача однієї країни можуть використовувати треті особи з будь-якого куточка світу.

В Україні питання захисту персональних даних регулюється Законом України «Про захист персональних даних», який набрав чинності у 2011 р. [1].

Принципами обробки персональних даних в Україні є відкритість і прозорість, відповідальність, адекватність, не надмірність їх складу та змісту стосовно визначеної мети обробки, а також підстави для обробки персональних даних – згода суб'єкта персональних даних.

Актуальність обраної теми полягає в тому, що у багатьох суб'єктів підприємницької діяльності та фізичних осіб доволі низький рівень правової освіченості у сфері захисту персональних даних. З кожним роком обіг інформації збільшується, полегшується доступ до всіляких інтернет-ресурсів, а отже є ймовірність того, що будь-хто може неправомірно заволодіти інформацією про ту, чи іншу особу, якщо не вживати засобів захисту.

Вже більше 10 років проблема захисту персональних даних знаходяться у центрі уваги вітчизняних науковців і практиків. Наразі питання захисту персональних даних є актуальним для всіх підприємств і організацій, для державних установ, які своєю діяльністю узагальнюють та використовують інформацію про особу. Відповідно Закону України «Про захист персональних даних», Закону «Про захист інформації в інформаційно-телекомунікаційних системах» та численних нормативних актів, така інформація повинна бути захищена від модифікації, несанкціонованого доступу та розповсюдження [2].

Проект захисту персональних даних на прикладі окремо взятого підприємства – ТОВ «ПФСОФТ» передбачає що необхідно усвідомлювати важливість захисту персональних даних, обґрунтовувати це всім зацікавленим сторонам, аналізувати ризики недотримання законодавчих вимог, визначити та

врахувати у сумі загальних витрат – витрати на вдосконалення системи захисту персональних даних. Враховувати його можливий вплив на поточну діяльність підприємства.

Метою кваліфікаційної роботи є створення моделі системи захисту персональних даних на прикладі конкретного підприємства.

Для досягнення мети слід вирішити ряд завдань:

- розглянути існуючі та діючі в Україні та країнах ЄС стандарти захисту персональних даних;

- дослідити загрози, які можуть існувати щодо персональних даних

- ознайомитись з існуючими на підприємстві системами захисту даних;

- детально розглянути засоби апаратного та програмного захисту;

- дослідити та створити у разі необхідності особисту систему захисту персональних даних.

Об'єкт розробки: процес захисту персональних даних на підприємстві ТОВ «ПФСОФТ».

Предмет розробки: система захисту персональних даних на підприємстві ТОВ «ПФСОФТ».

Методи дослідження: аналіз існуючих систем та засобів захисту персональних даних.

Практична цінність. Удосконалення системи захисту персональних даних на підприємстві, що призведе до поліпшення захисту особистої інформації, завдяки тому, що було удосконалено методи програмного та апаратного захисту системи. Дана система може бути використана на практиці іншими підприємствами і організаціями.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Основним законом нашої країни є Конституція. Статтею 32[3] Конституції України передбачено декілька гарантій у сфері захисту персональних даних: конфіденційна інформація про особу не може збиратися, зберігатися, використовуватися та поширюватися без її згоди, крім випадків, передбачених Конституційним законом України, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Особливу гостроту питання захисту персональних даних набрало останнім часом, коли все більше людей почали користуватися Інтернетом, стрімко розвиваються соціальні мережі. Уперше тема захисту особи прозвучала в Загальній декларації прав людини, прийнятій на третій сесії Генеральної Асамблеї ООН і підписаній 10 грудня 1948 року. У Декларації зазначено, що ніхто не може зазнавати необґрунтованого втручання в його особисте і сімейне життя, недоторканість його сім'ї, таємницю листування, честь і репутацію; і що кожен має право на захист від такого втручання або напади. Слід, однак, зазначити, що ця норма не використовується громадянами спеціально для захисту своїх прав. Згодом Конвенція «Про захист прав людини і основоположних свобод»[4], підписана 4 листопада 1950 року (ратифікована Україною 17 липня 1997 року із заявами та застереженнями, набула чинності 11 вересня 1997 року), стаття 8 приблизно повторює тими ж словами «кожен має право на повагу до свого приватного і сімейного життя, житла і кореспонденції». Єврокоди — це не незмінний перелік документів, а фундаментальні принципи, відображені в документах, розроблених відповідно до політичних реалій і рівня технологічного розвитку.

Сьогодні питання захисту персональних даних є дуже важливим для всіх суб’єктів підприємницької діяльності, незалежно від форми власності, підпорядкованості, виду діяльності тощо, які узагальнюють та використовують

інформацію про особу. Дія Закону України «Про захист персональних даних» поширюється на фізичних та юридичних осіб, які здійснюють будь-яку дію або комплекс дій, таких як збір, реєстрація, накопичення, зберігання, адаптація, зміна, оновлення, використання та розповсюдження (розповсюдження, впровадження, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

Українське суспільство наразі потребує підвищення правосвідомості щодо захисту персональних даних. Проекти із захисту персональних даних передбачають необхідність усвідомлення важливості захисту персональних даних у компанії, обґрунтування цього для всіх зацікавлених сторін, аналіз ризику невідповідності вимогам законодавства, визначення орієнтовної вартості та графіку проекту та розрахувати його можливий вплив на вплив поточної діяльності компанії та вибрати найкраще рішення.

1.2 Формулювання вимог до системи захисту персональних даних

1.2.1 Поняття персональних даних

Так що ж означає термін «персональні дані», яка інформація може належати до них? Посилання на цей термін містять відразу 2 нормативно-правових акта: Закони України «Про захист персональних даних» [2] (далі – Закон) та Закон «Про інформацію» (далі – Закон про інформацію). Проаналізувавши їх, найбільш логічним буде висновок, що персональні дані (відомості про фізичних осіб) – це відомості або сукупності відомостей про ідентифіковану фізичну особу, або особу, яка може бути конкретно ідентифікована.

Отже, виходячи з терміну, визначеному у нормативних документах поняття «персональні дані» складається з декількох частин: «відомості чи сукупність відомостей»; «фізична особа»; «ідентифікована або може бути конкретно ідентифікована».

ВІДОМОСТІ ЧИ СУКУПНІСТЬ ВІДОМОСТЕЙ про особу можуть мати об'єктивний або суб'єктивний характер. Таких як об’єктивна інформація: аналіз крові людини, електрокардіограма, зафіксована в відомості зарплата тощо. Суб’єктивна інформація, наприклад опис посади. Зміст інформації може відображати приватне чи сімейне життя чи кар’єру людини. Тобто це може бути інформація, що стосується трудових відносин та соціальної поведінки, або інформація, яка вказує на те, що замовником чи виконавцем є фізична особа. Водночас, незалежно від сфери, у якій відносини, що підлягають обробці, породжують персональну інформацію, така інформація є персональними даними. Окремо виділяється так звана «чутлива інформація». Закон «Про захист персональних даних» встановлює особливі вимоги щодо обробки окремих категорій персональних даних. Це інформація про расу, етнічне походження, політику, релігію, світоглядні переконання, стан здоров'я, статеве життя, членство в політичних партіях, профспілках. Інформація може стосуватися прямо чи опосередковано фізичних осіб. Прямий - Наприклад, це конкретна особиста ситуація про людину, або банківський рахунок з номером, ідентифікаційним кодом конкретної людини. Однак часто бувають ситуації, коли інформація опосередковано стосується нас. Наприклад, ведеться реєстр нерухомого майна, власник нерухомості та особа, яка надає послуги чи ремонт, – усі пов’язані з майном. Опосередковано ця інформація стосується і цих людей.

«…ІДЕНТИФІКОВАНА АБО МОЖЕ БУТИ КОНКРЕТНО ІДЕНТИФІКОВАНА» Особу можна ідентифікувати як прямо, так і опосередковано. Якщо на будь-якому документі вказано прізвище, ім’я, по батькові чи будь-яка інша інформація, дата народження, фотографія, місце народження, то, звичайно, особу можна ідентифікувати безпосередньо. Закон про захист персональних даних містить таку фразу: «може бути конкретно ідентифікована». При визначенні можливості ідентифікації особи необхідно враховувати всі можливі способи її ідентифікації. Перед початком обробки

персональних даних особа, яка обробляє персональні дані, повинна визначити, які дані вважатимуться персональними.

При розгляді поняття персональних даних неможливо обійтися без розуміння того, хто є суб'єктами відносин, пов'язаних із персональними даними? Хто, власне, обробляє персональні дані? Закон України «Про захист персональних даних» вводить такі поняття:

- володілець персональних даних —у документах з питань захисту персональних даних Ради Європи та Європейського Союзу — «контролер, англійською controller» — Юридичні або фізичні особи, які обробляють персональні дані від свого імені. Це може бути організація або фізична особа: підприємець, юрист, лікар, будь-хто, крім тих, хто обробляє персональні дані в особистих побутових цілях. Власнику важливо визначити мету, визначити, що є персональними даними та процедури їх обробки.
- розпорядник персональних даних — Фізичні або юридичні особи, уповноважені індивідуальним власником бази даних або законом на обробку цих даних. Розпорядник (у документах Європейської комісії та ЄС щодо захисту персональних даних — процесор, англійською — processor) самостійно не визначає цілі обробки персональних даних, її склад та процедури обробки. Розпорядник діє від імені власника, який визначив цілі, для яких контролер обробляє персональні дані, визначає, що є персональними даними, і встановлює процедури обробки для контролера.
- Третя особа – крім суб’єкта персональних даних, власника або розпорядника бази персональних даних та уповноваженого державного органу з питань захисту персональних даних, будь-яка особа, якій власник або розпорядник бази персональних даних передає персональну інформацію, обробляється відповідно до закону. Організацію можна ідентифікувати як третю сторону, якщо вона не є власником, контролером або органом захисту даних. У той же час треті особи також можуть бути власниками персональних даних або контролерами, які діють від імені інших власників у більшості випадків. З точки зору компаній, установ чи організацій, які є власниками баз

персональних даних та обробляють персональні дані працівників, місцевих органів влади, виконавчих органів Фонду соціального страхування від нещасних випадків, тимчасової втрати працездатності, соціального захисту інвалідів, пенсійного забезпечення, держпраці інспекція, служби зайнятості, податкові служби, прокуратура тощо є третіми особами, яким передаються окремі працівники у випадках, передбачених законом. Певні установи зобов'язані вживати заходів для забезпечення дотримання вимог законодавства про захист персональних даних.

Закон «Про захист персональних даних» [2] вводить ще поняття бази персональних даних як іменованої сукупності упорядкованих персональних даних в електронній формі та/або у формі картотек.

Водночас сучасне життя людини неможливе без надання інформації про себе іншим членам суспільства та державним органам. Як зазначено в ст. 2 Закону України «Про інформацію» від 2 жовтня 1992 р. [5] кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання і захисту інформації, необхідної для здійснення його діяльності. права, свободи та інтереси. Широке поширення та використання інформаційних технологій, глобальних інформаційних систем та автоматизованих баз даних значно полегшує громадянам реалізацію цього права. Але, незважаючи на всі переваги, є один серйозний недолік - високий ризик несанкціонованого втручання в особисте життя і зловживання «приватними» даними.

Першою проблемою, з якою зіткнулися менеджери персональних даних під час реєстрації в загальнодержавному реєстрі баз персональних даних, було визначення того, яка інформація є персональними даними, а яка ні. Відповідно до ст. 11 Закону України «Про інформацію» від 2 жовтня 1992 р. У роз'ясненнях Мін'юсту «Деякі питання практичного застосування Закону України «Про захист персональних даних» від 21 грудня 2011 р. вказується, що законодавством України не встановлено і не може встановлюватися перелік відомостей про фізичну особу, які є персональними даними, для можливості

застосування правових норм у різних ситуаціях, у тому числі при обробці персональних даних в (автоматизованих) базах даних та внесенні персональних даних системи, які можуть з'явитися в майбутньому в результаті технологічної, соціальної, економічної та інших сфер суспільного життя, визнаючи наявність проблеми, не дали відповіді на питання, яка інформація дозволяє ідентифікувати людину [5].

Веб-сайт державної служби України з питань захисту персональних даних також не дав конкретної відповіді на це питання, а лише припустив, що визначення слова «персональні дані» в Законі України «Про захист персональних даних» повністю відповідає положенням Ради Європейської конвенції про захист персональних даних Визначення встановленого строку Обробка персональних даних [6].

Конституційний Суд України формально тлумачить частини першу та другу статті 32 Конституції України, вважаючи, що відомостями про особисте та сімейне життя особи (персональні дані про неї) є відомості про особу або сукупність відомостей, які встановлені або особа, яку можна конкретно ідентифікувати, а саме: громадянство, освіта, сімейний стан, віросповідання, стан здоров'я, фінансовий стан, адреса, дата та місце народження, проживання та місце перебування тощо. Дані про зв'язок з іншими людьми (особливо з членами сім'ї), особисті майнові та позашлюбні відносини та відомості про події та явища, що мали або мають місце у повсякденній, інтимній, соціальній, професійній, діловій та інших сферах життя. Зазвичай персональні дані, які надає особа, стосуються її вступу в якісь правовідносини (професійні, цивільні, економічні тощо). Право на використання персональних даних ґрунтується на згоді суб'єкта даних на їх обробку, як зазначено в частині першій статті 11 Закону.

Тобто, з одного боку, законодавець надає право особам давати згоду на використання їх персональних даних, а з іншого – передбачає адміністративну та кримінальну відповідальність володільців персональних даних за використання їх персональних даних без згоди. згоден. Наприклад, відповідно

до ст. 24 КЗпП України передбачено, що при укладанні трудового договору громадяни пред'являють паспорт або інші документи, що посвідчують особу, трудову книжку, а у випадках, встановлених законодавством, документи про освіту (професію, кваліфікацію), документи військкомату тощо. [7].

Це питання стає актуальним з іншого боку. У зв'язку з посиленням заходів відповідальності за порушення роботодавці активно вимагають від працівників згоди на використання персональних даних, які вони вже отримали під час працевлаштування. Більшість співробітників майже автоматично підписують такі угоди, тим самим погоджуючись на використання персональних даних. При цьому фізичні особи зберігають усі права, встановлені законом, щодо своїх персональних даних. У деяких випадках відмова у згоді на використання персональних даних не забезпечує можливості реалізації прав та обов'язків цієї ж особи. Наприклад, обробка персональних даних працівників для реалізації прав та обов'язків у трудових відносинах, контролю та сплати податків без згоди працівників. Тому у виняткових випадках закон має передбачати можливість обробки персональних даних, необхідних для укладення та виконання договору, без згоди суб'єкта даних.

Надаючи роботодавцям право отримувати розширену інформацію про персональні дані працівників, закон зобов'язує роботодавців вживати всіх заходів для запобігання несанкціонованому вилученню такої інформації з ведення роботодавця, щоб персональні дані працівника не стали власністю третьої особи без його відома. і за згодою.

Аналізуючи поняття персональних даних, слід звернути увагу на те, які можна виділити категорії відомостей персональних даних:

– за природою – об'єктивні та суб'єктивні відомості про фізичну особу

– за джерелами – відомості, що отримані з первинних (загальнодоступні джерела, від самої особи і т. п.) або вторинних джерел (наприклад, з іншої бази персональних даних);

– за способами обробки – текстові (цифрово-буквені), графічні відомості, відомості у відео форматі тощо;

– за носіями – на папері або в електронній формі;

– за «правовим режимом» – відомості, до яких застосовуються загальні або особливі норми;

– за ступенем зв'язку з особою – дані, що стосуються її безпосередньо або опосередковано;

– за терміном обробки (зберігання) – короткострокові (до 3 років), середньострокові (до 10 років), довгострокові (70 років або більше) та безстрокові (довічно);

– за змістом – ідентифікаційні дані, паспортні дані; особисті відомості склад сім'ї, освіта, професія, біометричні або психологічні, житлові умови, спосіб життя, життєві інтереси та захоплення, споживчі звички, фінансова інформація, електронні ідентифікаційні дані, електронні дані про локалізацію, запис зображень, звукозапис, інші;

– за суб'єктним складом – відомості громадян, найманих працівників, посадових осіб, платників податків та зборів тощо.

При розгляді поняття «Персональні дані» слід приділити увагу не тільки захисту інформації про працівника, а й захисту інформації (роботодавця (конфіденційність).

В ІТ-діяльності компанії поняття «конфіденційність» може мати багато аспектів, тому питання захисту приватності також є багатогранним. Під час проведення корпоративних заходів важливо запобігти розголошенню унікальної клієнтської бази або злому серверів, можливості залишити в таємниці проект, який тільки розробляється, але підриває ринок, тощо. Тому знання шляхів і способів захисту конфіденційної інформації компанії, в тому числі захисту персональних даних, є одним із запоруок її успішної діяльності.

Таким чином, збереження персональних даних в ІТ компанії ТОВ «ПФСОФТ», а саме: клієнтської бази, персональних даних фізичних осіб, унікального софту, алгоритмів роботи та інших може у багато разів перевищувати вартість їх матеріальних активів (офісне приміщення, обладнання, техніка тощо).

У разі розголошення конфіденційної інформації, персональних даних втрати компанії в моменті можуть бути колосальними, не кажучи про втрати в перспективі.

1.2.2 Аналіз існуючих загроз та їх джерел для безпеки персональних даних на підприємстві

Ми живемо в епоху стрімкого розвитку інформаційних технологій, за допомогою яких люди можуть отримувати будь-яку інформацію, тим самим відкриваючи шлях до нових можливостей і отримання знань. Але ці можливості створюють загрозу безпеці, свободі та приватному житті людей. Країни по всьому світу стикаються з загрозами персональним даним і витоку конфіденційної інформації. Більшість ризиків пов'язана з крадіжкою персональних даних. Згідно з дослідженням [8], загроза витоку персональних даних посідає друге місце серед основних бізнес-загроз. Загрози безпеці - це певний набір умов або факторів впливу, що створюють небезпеку стосовно персональних даних.

За можливим характером загроз цілісності та конфіденційності персональних даних, що зберігаються у відповідних базах, їх можна умовно поділити на такі види:

– неавторизований доступ до

– незаконне ознайомлення з персональними даними

– модифікація або знищення

– відмова у послугах чи у використанні даних відповідно до визначених цілей

– доступ до даних від імені підставної персони або відмова від авторства доступу до персональних даних

– неавторизоване управління базою персональних даних

Джерелом загроз безпеці персональних даних можуть бути як внутрішні зловмисники, а саме власні співробітники, так і зовнішні зловмисники, які використовують для здійснення погроз канали зв'язку, комп'ютерні мережі та Інтернет.

Крім того, загрози безпеці можуть виникнути, коли в інформаційні системи потрапляють шкідливі програми та віруси. Несанкціонований доступ до інформації, розголошення через технічні канали та спеціальний вплив на персональні дані чи інформаційні системи – все це може бути вектором загроз безпеці.

Загрозу несанкціонованого доступу до персональних даних, що обробляються в інформаційних системах, можна подолати за допомогою апаратних, програмних і програмних засобів. У таких випадках порушуються режими конфіденційності шляхом незаконного копіювання та/або розповсюдження персональних даних.. Крім того, захищені особисті дані можуть бути змінені або знищені порушниками, що також може мати значні наслідки. Коли реалізується загроза несанкціонованого доступу, можуть створюватися аномальні режими роботи операційного середовища або програмного забезпечення, які зловмисник може використовувати для викрадення інформації або впливу на неї звідти. Реалізуючи загрози безпеці, зловмисники можуть скористатися різними вразливими місцями, включаючи недостатні рівні захисту, недосконале системне та прикладне програмне забезпечення, а також мережеві протоколи для зв'язку інформаційної системи.

Іншим видом загрози безпеці персональних даних є загрози, реалізовані через технічні канали, такі як витік мови, специфічна інформація, що містить персональні дані, персональні дані, оброблені інформаційними системами, витік через канали електромагнітного випромінювання та перешкод тощо. Крім того, захищені особисті дані можуть бути змінені або знищені порушниками, що також може мати значні наслідки. Коли реалізується загроза несанкціонованого доступу, можуть створюватися аномальні режими роботи

операційного середовища або програмного забезпечення, які зловмисник може використовувати для викрадення інформації або впливу на неї звідти.

Ці загрози, як правило, вважаються пов'язаними з інформаційними системами вищого рівня, які обробляють спеціальні категорії персональних даних, пов'язаних з етнічною та расовою приналежністю, релігійними чи філософськими переконаннями, здоров'ям і приватним життям особи. Відповідно до законодавчих вимог розроблено спеціальну модель загроз інформаційної системи, під час компіляції проаналізовано окремі уразливості та загрози, їх актуальність, адекватність наявних уразливостей та загроз та необхідність розрахунку додаткових методів і засобів захисту. Надаючи свої персональні дані для зберігання, використання, модифікації тощо, суб'єкт очікує, що вони будуть захищені від несанкціонованого доступу, використання, поширення та знищення.

Для забезпечення безпеки оператори ПД повинні розробити систему протидії атакам зловмисників, для цього спочатку необхідно визначити, кого і якої поведінки побоюватися. Світова практика показує, що найбільш ефективним є СЗПД, засноване на детальному створенні загрози. Щоб визначити фактори, які можуть призвести до порушення безпеки, ви можете лише ідентифікувати загрози персональним даним та їх походження. Будь-яка організація, приватне підприємство чи окрема особа, чия діяльність пов'язана з обробкою приватної інформації громадян, ризикує спробами зловмисників отримати, змінити, знищити чи передати її третім особам без належного дозволу власника.

В рамках функціонування інформаційної системи персональних даних (ІСПД) загрози персональних даних - це всілякі умови і чинники, здатні за певних обставин викликати їх витік або неправомірне використання або вплив. Крім очевидних випадків, таких як промислове шпигунство, ця категорія також включає ситуації, коли сторонні співробітники підприємства поширюють інформацію або передають конфіденційну інформацію без їх відома.

Завданням керівництва, а точніше уповноваженого персоналу чи відповідних експертів є виявлення «дірок» у системі безпеки ПЗ та вжиття заходів щодо їх усунення в майбутньому. Важливо розуміти, що виявлення загроза безпеки персональних даних (ЗБПД) не обов'язково означає крадіжку або втрату даних. Це означає, що можуть виникнути небезпечні ситуації, яких слід уникати. Для кожної існуючої інформаційної системи ПД необхідно створити конкретну модель факторів ризику. У той же час кількість ситуацій і поведінки, які можуть певним чином вплинути на його функціонування, величезна. Щоб полегшити ідентифікацію небезпек, їх класифікують за такими ознаками: За типом джерела. Вони виникають внаслідок властивостей використовуваних технічних засобів, природних явищ, дій осіб або третіх осіб за допомогою міжнародних і внутрішніх мереж.

Окрему групу становлять загрози ПД, викликані вірусами та апаратними закладками. Примітно, що немає чіткої інструкції щодо виявлення незадекларованих опцій, що змушує оператора робити це на свій страх і ризик. Найнадійніше використовувати ліцензійну серію програм, які отримали велику кількість позитивних відгуків експертів. Залежно від використовуваної реалізації. Можна оцінити фактори ризику через спеціальні впливи, витоки через технічні канали, через несанкціонований доступ.

За типом ІСПД. У цьому випадку замість детального переліку зазвичай проводиться віднесення в залежності від категорії споруди, що піддається небезпеці. Розрізняють УБ, пов'язані з операціями в локальній ІС, автоматизованому робочому місці та розподіленій системі. На підставі виконаних несанкціонованих операцій. Тут зазвичай виділяють загрози, які призводять до порушення конфіденційності ПД без прямого впливу на зміст інформації.

За уразливості. Прикладне програмне забезпечення системи, мережеві протоколи обміну, недостатня розвиненість технічних каналів і заходів захисту інформації можуть призвести до ризиків. Залежить від того, кого це стосується – автоматизованих робочих місць, мереж зв'язку, системного програмного

забезпечення, прикладних утиліт, коштів, що виділяються на обробку інформації.

Аналізуючи поняття персональних даних можна скласти одну із можливих класифікацій загроз для персональних даних:

- наслідки стихійних лих і техногенних катастроф;
- відмови обладнання;
- наслідки помилок проектування системи захисту;
- наслідки помилок персоналу;
- навмисні дії порушників.

Порушення режимів інформаційної безпеки можуть стати результатом спланованих дій зловмисників і недосвідчених співробітників. Користувач повинен принаймні мати деякі концепції інформаційної безпеки, які загрожують програмному забезпеченню, щоб його поведінка не загрожувала компанії та окремим особам. Такі невтішні обставини, як-от втрата або розголошення інформації, також можуть бути результатом цілеспрямованих дій співробітників компанії, які прагнуть отримати прибуток в обмін на цінні дані організації, в якій вони працюють або працювали, а також бездіяльності посадових осіб компанії. відповідає за забезпечення інформаційної безпеки.

Основними джерелами загроз є окремі зловмисники («хакери»), а також групи кіберзлочинців, які використовують усі доступні засоби. Щоб зламати захист і отримати необхідну інформацію, вони використовують слабкі місця та помилки в роботі програмного забезпечення та мережевих додатків, недоліки в налаштуваннях екрану мережі та прав доступу, вдаються до прослуховування каналів зв'язку та використання клавіатурних шпигунів. Типи атак, які можуть бути здійснені, залежать від типу інформації, місця розташування, методу доступу та рівня захисту. Якщо атака розрахована на основі недосвідченості посадових чи окремих осіб, то можливе, наприклад, використання спаму. Визначення каналів і причин несанкціонованого доступу та неправомірної поведінки має першорядне значення та повинно стати відправною точкою для побудови моделі безпеки персональних даних.

Всього є три типи джерел, кожен з яких має свої особливості:

1. Антропогенні. Особоивістю цього типу є те, що суб'єктів які мають можливість здійснювати операції з конфіденційною інформацією може бути декілька. У цю групу входять наступні джерела загроз персональних даних:

- Зовнішні - постачальники послуг, працівники контролюючих державних органів та аварійних служб, а також хакери, представники конкуруючих організацій. Їх дії можуть бути навмисними, тобто спрямованими на отримання відомостей, або неспеціальних, наприклад, якщо витік відбувається в результаті технічного збою або непрофесійного складання проекту інформаційної системи.

- Внутрішні - співробітники. В процесі своєї діяльності вони можуть піддавати системам захисту персональних даних ризикам через некомпетентність, помилки, застосування стороннього софту, спотворення і знищення компонентів програм, надання доступу неуповноваженим особам або ігнорування правила зберігання ПД. Причиною витоку може стати також самовільна зміна параметрів системи захисту і замовчування фактів.

2. Стихійні. Найбільш складно прогнозовані через розмаїття причин виникнення та способів прояву. Переважно це ті чинники, на які посадові особи, які є відповідальними за збереження персональних даних, ніяким чином не здатні вплинути, а саме:

- повені;
- цунамі;
- пожежі;
- урагани;
- зсуви;
- радіаційні катастрофи;
- військові конфлікти.

3. Техногенні. Ці джерела визначаються використовуваними технічними засобами і бувають двох видів: внутрішні – це апаратні закладки, віруси та інші шкідливі програми, системи безпеки та сигналізації, неякісне програмне та

апаратне забезпечення, задіяне в обробці персональних даних; зовнішні - елементи інфраструктури цілей, наприклад, телефонні та інтернет-лінії, опалення, каналізація, водопостачання, газові установки. Найпоширенішим способом пошкодження системи та викрадення даних є комп'ютерний вірус.

На даному етапі потрібно детально розглянути як працює кожен з вірусів та яку шкоду він може нанести.

Резидентні віруси. Під терміном "резидентність" (DOS'овскій термін TSR - Terminate and Stay Resident) розуміється здатність вірусів залишати свої копії в системній пам'яті, перехоплювати деякі події (наприклад, звернення до файлів або дисків) і викликати при цьому процедури зараження виявлених об'єктів (файлів і секторів). Таким чином, резидентний вірус активний не тільки під час роботи зараженої програми, а й після того, як програма завершила свою роботу. Резидентна копія такого вірусу зберігається до наступних 20 перезавантажень, навіть після знищення всіх заражених файлів на диску. Зазвичай неможливо видалити такі віруси шляхом відновлення копій файлів з дистрибутивних дисків або резервних копій. Резидентна копія вірусу залишається активною та заражає новостворені файли. Те саме стосується завантажувальних вірусів – форматування диска за допомогою резидентного вірусу в пам'яті не завжди виліковує диск, оскільки багато резидентних вірусів повторно заражають диск після форматування.

Нерезидентні віруси. Навпаки, нерезидентні віруси активні відносно короткий проміжок часу - тільки при запуску зараженої програми. Для їх поширення вони шукають на диску незаражені файли і записують їх. Після того, як код вірусу передає управління головній програмі, вплив вірусу на роботу операційної системи буде зведено до нуля до наступного запуску будь-якої зараженої програми. Таким чином, набагато простіше видалити з диска файли, заражені нерезидентним вірусом, і в той же час запобігти повторному зараженню вірусом.

Стелс-віруси. Стелс-віруси якимось чином приховують факт своєї присутності в системі. Використання алгоритму Stealth дозволяє вірусу

повністю або частково сховатися в системі. Найпоширенішим стелс-алгоритмом є перехоплення запитів ОС на читання/запис заражених об'єктів. При цьому стелс-вірус або тимчасово їх обробляє, або «замінює» неінфіковані області інформації. Для макровірусів найпопулярнішим методом є блокування викликів меню перегляду макросів. Відомі всі види стелс-вірусів, крім вірусів Windows - завантажувальних вірусів, файлових вірусів DOS і навіть макровірусів. Ймовірно, це лише питання часу, коли невидимий вірус заразить файли Windows.

Полиморфік-віруси. Майже всі типи вірусів використовують самошифрування та поліморфізм, щоб максимально ускладнити процес виявлення вірусів. Поліморфні віруси (polymorphic) досить важко виявити віруси, вони не мають сигнатури, тобто не містять постійних частин коду. У більшості випадків два зразки одного поліморфного вірусу не будуть збігатися. Це досягається шляхом шифрування тіла вірусу та модифікації процедури дешифрування. До поліморфних вірусів належать ті, які неможливо (або надзвичайно важко) виявити за допомогою так званих вірусних масок (частин постійного коду конкретного вірусу). Це досягається двома основними способами - шляхом шифрування основного коду вірусу за допомогою непостійного ключа та поєднання його з набором команд дешифрування або шляхом зміни виконуваного коду самого вірусу. Поліморфізми різного ступеня складності існують у всіх типах вірусів — від завантажувальних і файлових DOS-вірусів до Windows-вірусів.

За середовищем «проживання» віруси можна розділити на: файлові; завантажувальні; макровіруси; мережеві.

Файлові віруси. Файлові віруси або вводять себе у виконувані файли різними способами (найпоширеніший тип вірусу), створюють дублікати файлів (віруси-супутники) або використовують особливості організації файлової системи (віруси посилань). Майже всі виконувані файли всіх популярних операційних систем можуть вносити файлові віруси.

До теперішнього часу відомо, що віруси вражають всі типи виконуваних об'єктів стандартної DOS: командні файли (BAT), завантажувані драйвери (SYS, включаючи спеціальні файли IO.SYS і MSDOS.SYS) і виконувані двійкові файли (EXE, COM). Є віруси, які впливають на виконувані файли для інших операційних систем - Windows 3.x, 22 Windows95/NT, OS/2, Macintosh, UNIX, включаючи драйвери VxD для Windows 3.x і Windows95. Деякі віруси заражають файли, що містять вихідний текст програми, бібліотеки або об'єктні модулі. Можна записати вірус у файл даних, але це або наслідок помилки вірусу, або виникає, коли проявляється його агресивність.

Макро-віруси також записують свій код у файли даних - документи або електронні таблиці, - проте ці віруси настільки специфічні, що винесені в окрему групу.

Завантажувальні віруси. Завантажувальні віруси заражають завантажувальний сектор дискет і завантажувальний сектор або головний завантажувальний запис (MBR) жорстких дисків. Принцип дії вірусу-завантажувача заснований на алгоритмі запуску операційної системи при включенні або перезавантаженні комп'ютера - після виконання необхідних тестів на встановлених пристроях (пам'ять, диск і т.д.) програма запуску системи спочатку читає фізичний сектор завантажувального диска (A:, C: або CD-ROM, залежно від параметрів, встановлених у налаштуваннях BIOS) і передає йому керування. У випадку з дискетою або компакт-диском управління отримує завантажувальний сектор, аналізує таблицю параметрів диска (BPB - блок параметрів BIOS), обчислює адреси системних файлів операційної системи, зчитує їх в пам'ять і запускає їх виконання. Зазвичай системними файлами є MSDOS.SYS і IO.SYS, або IBMDOS.COM і IBMBIO.COM, або інші версії залежно від інсталяції DOS, Windows або інших операційних систем. Якщо на завантажувальному диску немає файлів операційної системи, програма, розташована в завантажувальному секторі диска, видає повідомлення про помилку та пропонує замінити завантажувальний диск. Для жорстких дисків керування отримують програми, розташовані в MBR жорсткого диска.

Ця програма аналізує таблицю розділів диска (Disk Partition Table), обчислює адресу активного завантажувального сектора (зазвичай цей сектор є завантажувальним сектором диска C), завантажує його в пам'ять і надає управління. Під контролем активний завантажувальний сектор жорсткого диска виконує ті самі операції, що й завантажувальний сектор дискети. При зараженні дисків завантажувальні віруси «замінюють» їх код, а не будь-які програми, які отримують управління при завантаженні системи. Таким чином, принцип зараження однаковий у всіх вищевказаних способах: вірус «змушує» систему запам’ятовувати і брати під контроль при перезавантаженні не вихідний код завантажувача, а код вірусу. Вінчестер заражається трьома можливими способами - вірус записується або замість коду MBR, або замість коду boot-сектора завантажувального диска (зазвичай диска C:), або модифікує адресу активного boot-сектора в Disk Partition Table, розташованої в MBR вінчестера.

Макро-віруси. Макро-віруси заражають файли документів і електронні таблиці кількох популярних редакторів. Макро-віруси — це програми, вбудовані в мову (макромова) деяких систем обробки даних (текстових редакторів, електронних таблиць тощо). Для розмноження такі віруси використовують можливості мови макросів і з їх допомогою переходять з одного зараженого файлу (документа або форми) в інший. Найпоширенішими вірусами стали макровіруси для Microsoft Word, Excel і Office. Існують також макровіруси, які заражають документи Ami Pro і бази даних Microsoft Access.

Мережеві віруси. До мережевих вірусів належать віруси, які активно використовують для поширення протоколи та можливості локальних і глобальних мереж. Основним принципом роботи мережевих вірусів є здатність самостійно передавати свій код на віддалені сервери або робочі станції. У той же час «складні» мережеві віруси також мають можливість запускати свій код на віддалених комп’ютерах або принаймні «підштовхувати» користувачів 24 до запуску заражених файлів.

Приклад мережевих вірусів - так звані IRCчерв'яки. IRC (Internet Relay Chat) - це спеціальний протокол, розроблений для комунікації користувачів

Інтернет в реальному часі. Протокол дозволяє їм «розмовляти» через Інтернет за допомогою спеціально розробленого програмного забезпечення. Окрім відвідування конференції, користувачі IRC мають можливість спілкуватися один на один з будь-яким іншим користувачем. Крім того, існує чимало команд IRC, за допомогою яких користувачі можуть отримувати інформацію про інших користувачів і канали, змінювати деякі налаштування IRC-клієнта тощо. Також є можливість відправляти і отримувати файли - на цій можливості заснований черв'як IRC. Виявляється, потужна і розгалужена система команд IRC-клієнта дозволяє створювати комп'ютерні віруси на основі скриптів, які передають свій код на комп'ютери користувачів мережі IRC, так звані «черв'яки IRC». Такі хробаки IRC працюють приблизно за тим самим принципом. За допомогою IRC-команд робочий файл сценарію (скрипт) автоматично надсилається із зараженого комп'ютера кожному користувачеві, який повторно приєднується до каналу. Надісланий файл сценарію замінює стандартний файл, і заражений клієнт знову надішле хробака під час наступної робочої сесії. Деякі хробаки IRC також містять компоненти троянського коня: вони виконують деструктивні дії на ураженому комп'ютері на основі заданих ключових слів. Наприклад, черв'як "pIRCH.Events" за командою стирає всі файли на диску користувача.

Існує багато комбінацій - наприклад, файловий завантажувальний вірус заражає файли і завантажувальні сектори диска. Такі віруси зазвичай мають досить складні алгоритми роботи, зазвичай використовують примітивні методи проникнення в систему, використовують стелс- і поліморфні методи тощо.

Теоретично, якщо система захисту побудована з урахуванням усіх сучасних методів і засобів захисту, а підприємство ретельно відбирає та навчає людей, які не допускають помилок, то в такій системі навмисні дії порушників практично неможливі. Однак на практиці це не завжди працює. Оскільки системи захисту з часом застарівають, персонал змінюється і втрачає пильність, зловмисники, хакери не стоять на місці, вони знаходять нові способи атак і способи подолання захисту, які були невідомі на момент розробки системи захисту.

Тому, маючи розумні очікування щодо стабільності системи захисту інформації, краще пам'ятати основне правило захисту інформації: жодна система захисту не може довгостроково протистояти цілеспрямованим діям кваліфікованих зловмисників із застосуванням сучасних технологій. Правила базуються на багаторічному досвіді експертів із захисту даних і є універсальними. Це не залежить від рівня захисту системи, чесності користувачів і адміністраторів, апаратного та програмного забезпечення. Мета захисту інформації, визначена в «Концепції захисту інформаційних технологій»: «Метою захисту інформації є запобігання або суттєве ускладнення загроз інформації про державну власність, з метою сприяння реалізації громадянами, юридичними особами та державними установами виконання покладених на них завдань і функцій законних інтересів на даний час, загрози, реалізація яких може завдати політичної, економічної, моральної та іншої шкоди державі, суспільству чи особам» [9].

1.2.3 Підходи до організації забезпечення захисту персональних даних

Конвенція про захист прав людини і основоположних свобод, прийнята в 1950 році, є основою захисту Європейським Співтовариством конфіденційної інформації, яка підпадає під категорію персональних даних. Крім того, Конвенція надає можливість лише в демократичному суспільстві захищати здоров'я та мораль або захищати права та свободи інших заради національної та громадської безпеки, економічного добробуту, нації та запобігання протиправних діянь чи злочинів [10]. Прийняття Міжнародного пакту про громадянські та політичні права в 1966 році продовжувало підтримувати концепцію міжнародного захисту персональних даних, викладену в Пакті.

Захист персональних даних – проблема, яка вже достатньо давно є актуальною не лише для українських компаній. Починаючи з 25 травня 2018 року в юридичному полі Європейського Союзу вступав в силу новий нормативний акт - Загальний Регламент Захисту Даних, більш відомий як

GDPR (General Data Protection Regulation) [11]. Євросоюз перейшов на нові правила поводження з персональними даними, а Регламент стосується будь-якої роботи з персональними даними, зокрема збору, зберігання, передачі. ТОВ «ПФСОФТ» здійснює зовнішньо-економічну діяльність і в своїй діяльності використовує різні підходи до організації забезпечення персональних даних , дотримуючись основних принципів обробки даних по GDPR

Загальний підхід європейців до обробки персональних даних викладений у вигляді 6 основних принципів[11]:

1. Законність, справедливість та прозорість. Персональні дані повинні оброблятися законно, справедливо та прозоро. Будь-яку інформацію про мету, методи та обсяги обробки персональних даних мається викладати максимально доступно та просто.

2. Обмеження застосування. Персональні дані повинні збиратися та використовуватись виключно з метою, що була заявлена компанією (або онлайн-сервісом).

3. Мінімізація даних. Забороняється збирати особисті дані в більшому обсязі, ніж той, що потрібен для досягнення мети обробки.

4. Точність. Особисті дані, які являються неточними, повинні бути видалені або виправлені (за вимогою користувача).

5. Обмеження зберігання. Особисті дані повинні зберігатися у формі, яка дозволяє ідентифікувати суб'єкти даних на строк не більше, ніж це необхідно для досягнення мети обробки

6. Цілісність та конфіденційність. При обробці даних користувачів компанія зобов'язана забезпечити захист персональних даних від несанкціонованої або незаконної обробки, знищення та пошкодження.

Чи необхідно використовувати систему захисту даних по GDPR у компанії ТОВ «ПФСОФТ», можна зрозуміти розглянувши схему, представлену на рис. 1.1.

Рисунок 1.1 – За яких умов вимагається слідування GDPR

Згідно цієї схеми (див. рис. 1.1), у випадку ТОВ “ПФСОФТ” норми GDPR не є обов’язковими, оскільки компанія ані має одиниці в ЄВ, ані сама не знаходиться в ЄС.

Існуючі системи захисту персональних даних - це дослідження різних процесів обробки персональних даних.

Також це аналіз документації, що стосуються організаційно-адміністративного напряму діяльності компанії, різноманітні пропозиції,

вдосконалення існуючих систем тощо. Аудит захисту персональних даних також може включати моніторинг існуючих систем у разі зміни законодавства або будь-яких загроз. Крім того, це можуть бути технічні заходи щодо створення системи захисту персональних даних. Аудит персональних даних продовжується експертним аналізом файлів. Для цього використовуються технічні, організаційні та розпорядчі документи. Необхідно пояснити технічну схему та різні функціональні схеми, а документацію перевірити на відповідність вимогам законодавства.

Важливо розуміти, для чого потрібно вжити заходи для захисту ПД. Якщо файл буде перевірено, навіть якщо частина інформаційної системи персональних даних не відповідає вимогам законодавства, то це буде підставою для відповідальності за фактом порушення вимог щодо захисту персональних даних. Наразі в процесі обробки персональних даних відносно вирішені відповідні питання, такі як стандартизація процесу збору персональних даних та забезпечення інформаційної безпеки, про що добре відомо більшості юристів.

Зрозуміло, що законодавство не є досконалим і потребує вдосконалення, але основні положення регулює Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI. Отже, відповідно до ст. Стаття 12 вищезазначеного закону визначає, що збір персональних даних є частиною їх обробки, яка передбачає відбір або систематизацію інформації про фізичних осіб. [1] Суб'єкт персональних даних поінформований про володільця персональних даних, склад і зміст зібраних персональних даних, права, передбачені законом, мету, з якою збираються персональні дані, та особу, якій його персональні дані передаються: дані, якщо вони були зібрані з персональних даних суб'єкта, в інших випадках – протягом тридцяти робочих днів з дати збору персональних даних. Окрім вищезазначеного Закону, юридичні та фізичні особи мають можливість вирішувати питання, пов'язані з власною інформаційною безпекою, використовуючи положення Цивільного кодексу України, Закону України «Про інформацію» та інших актів

українського законодавства [5]. З огляду на майбутні кроки України та євроінтеграційні амбіції, менш вивченим, але більш цікавим питанням є ознайомлення, дослідження та аналіз нормативних актів щодо захисту персональних даних, особливо щодо збору в країнах ЄС.

Питання захисту персональних даних та інформаційної безпеки в Інтернеті на даний момент є найбільш актуальним і активно розвивається. У результаті 25 травня 2018 року набули чинності нові правила захисту персональних даних в Інтернеті для користувачів, які знаходяться в Європейській економічній зоні (ЄЕЗ). Тут слід розуміти, що до ЄЕЗ входять не лише країни самого Європейського Союзу, а й країни Європейської асоціації вільної торгівлі (ЄАВТ), крім Швейцарії. Угода про створення Європейської економічної зони була підписана в 1992 році і набула чинності 1 січня 1994 року. ЄЕЗ базується на тих же «чотирьох свободах», що й Європейське співтовариство: вільний рух товарів, людей, послуг і капіталу між країнами ЄЕЗ. Тому існує режим вільної торгівлі між країнами ЄАВТ, які є членами ЄЕЗ та ЄС. Це дозволяє таким країнам ЄАВТ, як Ісландія, Норвегія та Ліхтенштейн, брати участь у єдиному європейському ринку без приєднання до ЄС.

Відповідно до Угоди про Європейську економічну зону розширення Європейського Союзу обов'язково веде до розширення Європейської економічної зони. Таким чином, ЄЕЗ наразі охоплює 30 країн. Нові правила, що називаються просто GDPR (Загальний регламент захисту даних), поширюються на всіх учасників глобальної мережі Інтернет, які збирають, зберігають або обробляють персональні дані. Хоча Закон було створено для захисту європейських даних, глобальний характер Інтернету означає, що GDPR встановлює стандарт конфіденційності даних у всьому світі. Майже всі великі інтернет-компанії, включаючи Google, Facebook і Twitter, підпадають під дію GDPR. GDPR має на меті забезпечити кращий захист особистих даних осіб, включаючи, але не обмежуючись, їхні релігійні чи політичні переконання. Штрафи за невідповідність величезні: до 20 мільйонів євро або 4% від загального обороту невідповідності. Крім того, GDPR надає користувачам вибір

засобів захисту від будь-яких матеріальних і/або нематеріальних порушень GDPR. GDPR поширюється на дані, які збираються, обробляються та/або зберігаються в Європі, незалежно від того, де дані були зібрані. Наприклад, якщо фізична особа володіє інтернет-магазином з розсилкою в Україні і на нього підписаний хоча б один потенційний клієнт з ЄС, то на такий інтернет-магазин поширюватимуться правила GDPR, що відкриває нові можливості для юристів у вдосконаленні знання та допомогу клієнтам. Важливою умовою GDPR є те, що з дати набрання чинності цим законом передача даних за межі ЄС до будь-якої країни, яка, на думку ЄС, не відповідає вимогам законодавства про захист персональних даних, забороняється. передає дані за межі ЄС для обробки або зберігання, тоді має бути отримана чітка згода користувача, який володіє даними [11].

У будь-якій ситуації, коли ви запитуєте дані користувача, спочатку запитайте себе: як це вплине на права власника даних? GDPR визначає наступні законні права, які мають власники даних: право на доступ, право на заперечення, право знати, право на виправлення, право на передачу даних, право на видалення, право не підлягати автоматичне прийняття рішень, а також право на обмеження обробки даних [11]. Однак власники даних також мають права. Наприклад, якщо користувач підписався на вашу розсилку. З часом він вирішив, що більше не хоче отримувати розсилку, і скасував підписку. У цьому випадку ви можете просто назавжди видалити електронну адресу користувача. Однак, коли користувачі підписуються на інформаційний бюлетень, вам потрібно знати їхню IP-адресу, щоб відповідати їхній згоді на отримання інформаційного бюлетеня (і ви повинні), оскільки ви маєте право зберігати ці дані, щоб підтвердити, що ваш сайт відповідає GDPR.

Важливо розуміти, що регулятори ЄС не повинні доводити ваше порушення. Це ваша юридична відповідальність - продемонструвати, що ви виконуєте вимоги, невиконання цього само по собі є невідповідністю. Ви також повинні вийти за рамки принципу конфіденційності за замовчуванням: користувачам не потрібно виконувати жодних дій для забезпечення

конфіденційності. Якщо користувачі нічого не зроблять, їхні дані будуть вважатися конфіденційними.

Слід розуміти, що у випадку, коли будь-яка з цих вимог суперечить згоді, яку ви отримали від своїх користувачів, вважатиметься, що ви не дали згоди, незалежно від намірів ваших користувачів. Крім того, GDPR спеціально вимагає спеціального повідомлення про конфіденційність [11]. Під захистом персональних даних розуміють комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки та конфіденційності персональних даних, що обробляються в ІСПД та поза ним.

Перед початком обробки персональних даних оператор зобов'язаний повідомити уповноважений орган із захисту прав суб'єктів персональних даних про намір здійснювати обробку персональних даних, за винятком:

1) відносяться до суб'єктів персональних даних, яких пов'язують з оператором трудові відносини;

2) отриманих оператором у зв'язку з укладенням договору, стороною якого є суб'єкт персональних даних, якщо персональні дані не поширюються, а також не надаються третім особам без згоди суб'єкта персональних даних і використовуються оператором виключно для виконання зазначеного договору та укладення договорів з суб'єктом персональних даних;

3) що відносяться до членів (учасників) громадського об'єднання чи релігійної організації та оброблюваних відповідними громадським об'єднанням або релігійною організацією, для досягнення законних цілей, передбачених їх установчими документами, за умови, що персональні дані не будуть поширюватися без згоди в письмовій формі суб'єктів персональних даних;

4) є загальнодоступними персональними даними;

5) включають в себе тільки прізвища, імена та по батькові суб'єктів персональних даних;

6) необхідних з метою одноразового пропуску суб'єкта персональних даних на територію, на якій знаходиться оператор, або в інших аналогічних цілях.

На етапі обстеження інформаційних систем ПД виконуються наступні роботи:

- формується перелік ПД, інформаційних систем і технічних засобів, що використовуються для їх обробки;

- визначаються підрозділи і працівники, які оброблятимуть ПД;

- визначаються категорії ПД; 31

- розробляється опис об'єкта захисту, включаючи склад і характеристики засобів обробки даних;

- проводиться попередня класифікація інформаційних систем ПД (перегляд класу проводиться на розсуд оператора в будь-який час);

- здійснюється оцінка необхідних заходів і витрат по приведенню інформаційних систем ПД у відповідність з вимогами.

Результатами робіт на етапі обстеження є:

- перелік ПД і категорії ПД;

- переліки інформаційних систем і технічних засобів, що використовуються для обробки ПД, і аналіз їх стану;

- склад наявних заходів і засобів захисту ПД;

- перелік підрозділів і співробітників, що обробляють ПД;

- класифікація інформаційних систем, що обробляють ПД на типові спеціальні; - акти класифікації інформаційних систем, що обробляють ПД;

- опис об'єктів захисту;

- уточнення типові моделі загроз і вимоги до систем захисту ПД;

- перелік необхідних заходів і орієнтовна вартість робіт по приведенню інформаційних систем ПД у відповідність з вимогами.

Залежно від способу зберігання (паперовий, електронний носій) персональні дані повинні оброблятися таким чином, щоб виключити доступ третіх осіб. З метою забезпечення безпеки персональних даних, що обробляються власниками, розпорядниками, вживаються спеціальні технічні заходи захисту, у тому числі виключення несанкціонованого доступу до персональних даних, що обробляються, та функціонування технічно-

програмних комплексів, за допомогою яких здійснюється обробка персональних даних. здійснюється. Отже, у разі обробки персональних даних необхідно створити належні умови для їх захисту.

1.2.4 Існуючи засоби забезпечення захиту персональних даних

ТОВ «ПФСОФТ», як і інші суб'єкти підприємницької діяльності всстановлюють технічні та організаційні заходи безпеки для забезпечення конфіденційності та цілісності персональних даних з метою захисту 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.

Зокрема, організація робочих процесів на підприємстві є дуже важливою для захисту персональних даних. Ключовим процесом є розробка документації, що включає:

- інформацію про дані, які збираються,
- мету обробки даних,
- порядок доступу до даних.

Не секрет, що у сфері ІТ, в цілому, так і на ТОВ «ПФСОФТ», персонал якому надається доступ до роботи з персональними даними, переважно ділиться на зовнішніх підрядників (ФОП та юридичних осіб) та офіційно оформлених працівників. На підприємстві складаються угоди про нерозголошення конфіденційної інформації, уважно складаються посадові інструкції працівників. Договори із зовнішніми підрядниками обов'язкого містять розділ стосовно обов'язків і вимог щодо нерозголошення даних.

На це питання варто звернути особливу увагу, адже саме людський фактор стає причиною дуже багатьох провалів у захисті та витоків інформації. Тим паче коли мова йде про працівників, відповідальних за підтримку безпеки персональних даних.

На підприємстві з періодичністю, яка зазначена у наказах керівника проводяться наступні заходи:

- аналіз чутливості персональних даних,
- обираються сфери регулювання та вимоги до захисту,
- проводиться експертиза діяльності зовнішніх провайдерів послуг і договорів із ними,
- при необхідності укладаються договори зі сторонніми організаціями стосовно консультацій з питань законодавства у сфері технічного і криптографічного захисту інформації
- розробляються та удосконалюються внутрішні документи на підприємстві,
- проводиться внутрішній аудит договорів і посадових інструкцій.

Далі більш детально було розглянуто засоби захисту персональних даних.

Фізична безпека. Фізична безпека об'єктів - стан захищеності життєво важливих інтересів (об'єктів) від загроз, джерелом яких є протиправні (несанкціоновані) злочинні дії фізичних осіб (порушників). Це включає захист об’єктів, обладнання від нещасних випадків або форс-мажорних обставин. Концепція безпеки - це загальна ідея захисту об'єктів від передбачуваних загроз.

Вразливість (об’єкта) – ступінь, до якого вжиті заходи захисту (об’єкта) не відповідають прогнозованим загрозам або заданим вимогам безпеки. Надзвичайна ситуація (на об'єкті) - це стан, при якому (на об'єкті) порушуються нормальні умови життя і діяльності людей, що створює загрозу їх життю і здоров'ю, завдає шкоди майну та навколишньому природному середовищу.

Ефективність системи фізичної безпеки – це ймовірність виконання системою своєї основної цільової функції – забезпечення захисту об’єктів від загроз, джерелом яких є протиправне (несанкціоноване) злочинне діяння фізичної особи (агресора). «Система фізичного захисту» — сукупність правових норм, організаційних заходів та інженерно-технічних рішень, розроблених для захисту життєво важливих інтересів і ресурсів підприємств

(об'єктів) від загроз, джерелом яких є фізичний вплив злочинів, вчинених фізичними особами (несанкціонованими особами).)- Порушники (терористи, злочинці, екстремісти тощо).

Сучасна СФЗ базується на широкому застосуванні інженерних та програмних засобів і складається з наступних основних компонентів (підсистем): - системи контролю та управління доступом персоналу; - системи охоронної сигналізації (SOS); - системи телевізійного спостереження (ТСН); системи оповіщення. - Системи забезпечення (освітлення, електропостачання, аварійне освітлення та ін.). При створенні сучасної СФЗ зазвичай також стоїть завдання захисту життєво важливих центрів і систем об'єкта від ненавмисних, помилкових або невмілих дій персоналу, які можуть завдати шкоди наближенням до НСД зовнішніх порушників. Враховуючи складність розв’язуваних завдань, створення важливих об’єктів СФЗ не може базуватися на принципі «розумної достатності», який часто використовується на практиці, а потребує комплексного наукового підходу. Такий підхід має на увазі проектування СФЗ важливих об'єктів в дві стадії: - концептуальне (системне) проектування; - робоче проектування.

Основними етапами стадії концептуального проекту є:

1) Аналіз вразливості об'єкта та існуючої СФЗ;

2) Розробка принципів фізичного захисту об'єкта;

3) Розробка техніко-економічного обґрунтування створення СФЗ.

Логічна безпека. Це включає заходи щодо ідентифікації та перевірки осіб або користувачів, які мають право доступу та зміни персональних даних. Логічна безпека стосується процесу використання програмних методів для перевірки прав користувача в певній комп’ютерній мережі чи системі. Ця концепція є частиною ширшої сфери комп’ютерної безпеки, яка включає апаратні та програмні методи захисту кінцевих точок або мереж. Обговорюючи логічну безпеку, розгляньте різні методи, які використовуються, включаючи імена користувачів і паролі, безпеку маркерів і взаємну автентифікацію в системі.

Автентифікація паролем, мабуть, найпоширеніший і звичний тип логічного захисту. Кожен, хто коли-небудь користувався сайтом онлайн-банкінгу або навіть системою соціальних мереж, буде знайомий з цією концепцією. Якщо мережу налаштовано на використання автентифікації за паролем, користувачі, які намагаються увійти до певного терміналу в мережі, повинні спочатку підтвердити свої облікові дані, ввівши ім'я користувача та пароль. Головною перевагою тут є простота, користувачам достатньо запам'ятати ім'я користувача та пароль для доступу до системи. Основним недоліком є те, що комп'ютери не можуть перевірити, чи користувач із певною комбінацією імені користувача та пароля є авторизованим користувачем; тому зловмисник може викрасти імена користувачів та паролі, щоб зламати систему.

Безпека токенів — це логічна техніка безпеки, яка передбачає використання карток-ключів або інших фізичних пристроїв для автентифікації користувачів у мережі. Після того, як користувач проводить свою картку в системі, йому надається доступ до комп'ютера. Деякі популярні типи пристроїв-токенів містять постійно змінювані коди, які перемикаються на нове значення щохвилини або близько того, захищаючи систему від спроб скопіювати картку безпеки. Знову ж таки, як і з автентифікацією за паролем, немає реального захисту від людей, які викрадають чужі картки доступу, щоб отримати доступ до системи.

Двостороння аутентифікація передбачає обмін запитаннями та відповідями між користувачем і комп'ютерною системою. Коли користувач намагається увійти в систему, комп'ютер надсилає запитання під назвою «завдання», на яке кінцевий користувач має відповісти правильним результатом, щоб отримати доступ до системи. Перевага цього методу логічної безпеки полягає в тому, що система не прив'язана до певної комбінації імені користувача та пароля; може виникнути стільки проблем, які перешкоджають легкому доступу неавторизованого користувача до системи, якщо конкретну комбінацію імені користувача та пароля викрадено.

Програми. Це одна з основних областей курсу захисту даних. Він представляє дозволи, якими повинна керувати система обробки персональних даних, щоб забезпечити належне використання даних, запобігаючи участі несанкціонованих користувачів, відокремлення середовищ та контроль контролю проникнення.

Програмна безпека – це захист інформації - спеціальна програмна система, що міститься в програмному забезпеченні для реалізації функції захисту інформації. Захисні програмні коди можуть запускатися самостійно як окремий захисний програмний продукт або включатися в комбінацію інших багатофункціональних програм з метою захисту даних, які вони обробляють, або захисту від шкідливого коду. Оскільки функції захисту багатофункціональних програм часто навіть не мають ефективних засобів самозахисту і за визначенням втрачаються для спеціалізованого програмного забезпечення захисту, будь-яка комп'ютерна система будь-якої важливості потребує розгортання та повністю інтегрованих елементів системи засобів захисту інформації програмного забезпечення.

Програмні засоби захисту інформації діляться на типи так:

- контроль доступу;
- анти-кейлоггери;
- анти-шпигуни (anti-spyware);
- анти-експлуататори (anti-subversion);
- анти-модифікатори (anti-tampering);
- антивіруси;
- шифрування;
- брандмауери (firewall);
- системи виявлення вторгнень;
- системи запобігання вторгнень;
- пісочниця;

Програмний захист інформації не слід плутати із захистом комп'ютерів від несанкціонованого використання або захистом комп'ютерних мереж, хоча

їхні функції багато в чому збігаються. При використанні цього методу захищається сама інформація, будь то операційна система, спеціалізоване програмне забезпечення або будь-яка цифрова форма документа. При цьому цей захист поділяється на захист даних і захист програм.

Комплексний програмний захист інформації на серверах або робочих комп'ютерах вимагає використання різних типів захисних програм або професійних захисних рішень, що поєднують кілька видів захисту одночасно. Наприклад, важливо розуміти, що поточні антивірусні підходи, які часто поєднують антивірус, антишпигунське програмне забезпечення, антиексплойти та антимодифікатори, є недостатніми проти цілеспрямованих атак, оскільки вони базуються на порівнянні програмного коду з шкідливий код підпису виробника. У деяких випадках можливість застосування аналізу поведінки також не гарантує збереження даних і збереження продуктивності системи. Крім того, контроль доступу сам по собі не гарантує, що програми та дані можуть використовуватися лише тими особами, які уповноважені на їх використання, оскільки, окрім уразливостей програмного забезпечення, цей тип захисту може бути «виявлений» звичайною соціальною інженерією без використання в принципі високого рівня.

Система виявлення вторгнень можуть допомогти в подальшому розслідуванні інциденту, але без системи запобігання вторгненням збиток від атаки може бути надто серйозним, щоб розслідувати його в першу чергу. Шифрування даних може допомогти запобігти спробам викрадення цих даних, але це не зупинить зловмисників, які хочуть їх знищити. Подібні недоліки вузькоспеціалізованого захисту можна знайти в будь-якій комбінації невеликої кількості схожих типів програмного забезпечення для захисту інформації, тому захист завжди має базуватися на багатьох паралельних і часто дублюючих алгоритмах. Коли використовується кілька рішень, це загрожує внутрішнім конфліктом системи, тому найбільш логічним висновком є використання складних систем безпеки, які використовують більшість згаданих типів захисту

інформації для захисту даних, захисту програм і самозахисту від вторгнення, копіювання, модифікація та знищення.

Усі програмні рішення безпеки SafenSoft мають модульну структуру та єдиний сервер керування, що гарантує можливість повної інтеграції в найскладнішу IT-інфраструктуру організації, одночасно захищаючи найменш захищені ділянки системи. Сумісність із встановленими рішеннями безпеки сторонніх виробників дозволяє усунути стандартну дилему побудови захищеної інфраструктури, тобто вибір того чи іншого рішення для виробництва, що гарантує клієнтам ефективність наших продуктів Проводити максимально об'єктивні оцінки за допомогою наших послуги із забезпечення інформаційної безпеки у своїх організаціях.

Шифрування. Це включає впровадження та використання алгоритмів шифрування, ключів, шифрів і спеціальних заходів безпеки для забезпечення цілісності та конфіденційності конфіденційних персональних даних у системі захисту даних. Шифрування даних є добре відомим і зрозумілим процесом. Обидві сторони використовують спеціальні ключі шифрування та дешифрування. Навіть якщо дані перехоплені зловмисником під час передачі інформації від відправника до одержувача, їх неможливо прочитати без ключа шифрування.

Тому перехоплення зашифрованої інформації стає безглуздим. Загальновідомо, що незважаючи на простоту шифрування даних як ідеї, практична реалізація ідеї представляє значні труднощі. Крипто, як і монета, має дві сторони. Небажано постійно використовувати надскладне шифрування даних, яке неможливо зламати, оскільки це створить великі труднощі для одержувача. Шифрування даних занадто простим ключем шифрування теж не дуже добре: трудомістко, безглуздо. У цьому випадку простіше взагалі не шифрувати. Всі розуміють, що будь-яка хороша система має бути збалансованою. Шифрування даних не є винятком: інформація та дані повинні надсилатися швидко, але в той же час дані повинні залишатися в безпеці.

Зараз віртуальна приватна мережа — VPN, яка використовує шифрування даних — є чудовим прикладом швидкого та безпечного підключення до Інтернету. VPN насамперед пов'язані з виявленням слабких місць у системах безпеки користувачів Інтернету та маскуванням IP-адрес великої кількості користувачів. Преміум-провайдери VPN приділяють максимальну увагу загальній безпеці своїх користувачів, а не лише забезпеченню безперервного з'єднання. На щастя, професіонали високого класу, які використовують шифрування даних для захисту вашої інформації, часто мають так багато доступних варіантів, що будь-якому зловмиснику набагато легше відмовитися від своїх планів, ніж продовжувати їх. Простіше кажучи, шифрування даних — це модифікація інформації, щоб зробити її невпізнанною для сторонніх. Як правило, шифрування даних відбувається за допомогою будь-якого методу шифрування або ключа шифрування/дешифрування (пароля), який відомий лише двом сторонам: відправнику та одержувачу. Шифрування цифрових даних складніше, ніж шифрування рукописного тексту, але базується на тих самих принципах. Існує два типи шифрування, кожен з яких використовує різні методи шифрування та дешифрування інформації. Найпоширенішим типом є симетричне шифрування даних, яке передбачає, що відправник і передбачуваний одержувач використовують той самий ключ для шифрування та дешифрування повідомлень.

Інший, більш складний тип шифрування даних називається асиметричним, коли відправник і одержувач використовують різні ключі для шифрування та дешифрування повідомлень. Шифрування даних перетворює передану інформацію на купу сторонніх символів, які не можуть бути прочитані та зрозумілі стороннім особам. Тільки ті, хто має ключ розшифровки, можуть ідентифікувати цю інформацію. Оскільки більшість даних, у тому числі медіа, відображаються як текст, їх можна зашифрувати таким же чином. Шифрування даних забезпечує конфіденційність будь-якого типу даних.

Мережевий зв'язок. Мережева модель даних - логічна модель даних, що є розширенням ієрархічного підходу, сувора математична теорія, що описує

структурний аспект, аспект цілісності і аспект обробки даних в мережевих базах даних. Мережевий зв'язок означає використання служб захисту даних компанії, включно з використанням систем моніторингу мережі, які постійно відстежують мережевий зв'язок і блокують будь-які підозрілі дії чи порушення безпеки. Ці аспекти програми навчання із захисту даних представляють мінімальні вимоги, тому компанії та/або організації повинні вжити додаткових неминучих заходів для забезпечення кращого захисту. Компанії повинні використовувати консультантів із захисту даних для впровадження систем захисту персональних даних. [12]

1.3 Висновки. Постановка задачі

Персональні дані є об'єктом підвищенної уваги різного роду шахраїв та зловмисників. Через незаконне заволодіння персональними даними можна нанести суттєву шкоду, як фізичній особі так і суб'єкту підприємницької діяльності. Спочатку треба виважено підійти до вивчення самого поняття «персональні дані», проаналізувати, яка інформація відноситься до персональних даних. Яка інформація може бути використана шахраями, і до яких наслідків це може призвести. Саме тому, грамотно створена система захисту персональних даних так чи інакше є дуже важливим.

Системи захисту потрібно постійно вдосконалювати, оновлювати. З часом, в системі захисту, в якій зберігаються ПД, з'являється все більше інформації, і треба прикладати більше зусиль для її збереження. І це не кажучи про те, що є і інші фактори, які впливають на захист. Саме тому в роботі було поставлено задачу створення та опису надійного захисту на основі вже існуючих систем.

Аналіз загроз показує, що небезпека може існувати у всьому: починаючи з дій або бездіяльності конкретних посадових осіб і закінчуючи природою, або форс – мажорними обставинами. Саме тому було прийнято рішення зібрати всі найкращі якості існуючих систем і об'єднати в одну.

Також, були проаналізовані підходи до організації забезпечення захисту персональних даних. Були представлені методи та засоби захисту, від фізичних до програмних. В наш час, в епоху стрімкого розвитку комп'ютерних технологій, розвинутій мережі інтернет дуже складно створити надійну систему захисту персональних даних. Тому керівництву підприємства, дуже важливо гарантувати своїм працівникам їх безпеку, що в свою чергу приведе до нерозголошення конфедінційної інформації про підприємство, про замовників та виконавцій, про укладені договори тощо, що в подальшому знайде відображення на прибутках підприємства, його конкурентоспроможності і його подальшого розвитку.

В розілі вже було розглянуто закони, які контролюють та забезпечують конфіденційність персональних даних. Також, було представлено підготовчий етап створення системи безпеки, у якій йдеться про попередній розгляд та класифікацію персональних даних, можливі загрози. У цьому розділі вже було розглянуто деякі засоби захисту.

У наступній частині роботи необхідно більш детально розглянути засоби апаратного та програмного захисту, переглянути вже існуючі системи захисту та розробити удосконалену систему захисту, яка дасть змогу ретельніше захищати персональну інформацію та персональні дані на підприємстві ТОВ «ПФСОФТ».

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про ТОВ «ПФСОФТ»

Дата державної реєстрації підприємства: 06.12.2006 р.

Підприємство розташовано за адресою: вулиця Мечнікова, будинок 10 Б, офіс 708, Центральний район, місто Дніпро, Дніпропетровська область, 49000.

З моменту державної реєстрації до теперішнього часу підприємство здійснює діяльність в галузі інформаційних технологій. Для здійснення діяльності підприємству відкриті наступні КВЕД:

62.09 Інша діяльність у сфері інформаційних технологій і комп'ютерних систем

58.29 Видання іншого програмного забезпечення

62.02 Консультування з питань інформатизації

63.11 Оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність

62.01 Комп'ютерне програмування

46.90 Неспеціалізована оптова торгівля.

Основними клієнтами товариства є нерезиденти, з якими укладені міжнародні контракти. Процес отримання замовлень та іх виконання відбувається шляхом віддаленого доступу. За межами митної території України. ТОВ «ПФСОФТ» є платником єдиного податку 3 групи за ставкою 5%.

Кількість штатних робітників на дату проведення обстеження складає 7 чоловік.

Графік роботи підприємства з понеділка по п’ятницю з 9-00 до 18-00 години.

Всі працівники підприємства є штатними. Їм нараховується заробітна плата та сплачуються податки.

На період дії воєнного стану в Україні робочі процеси на підприємстві застосовуються дистанційно, що находить відображення в наказі, який наведено у додатку Ґ.

На рис. 2.1 зображена організаційна структура підприємства ТОВ «ПФСОФТ»:

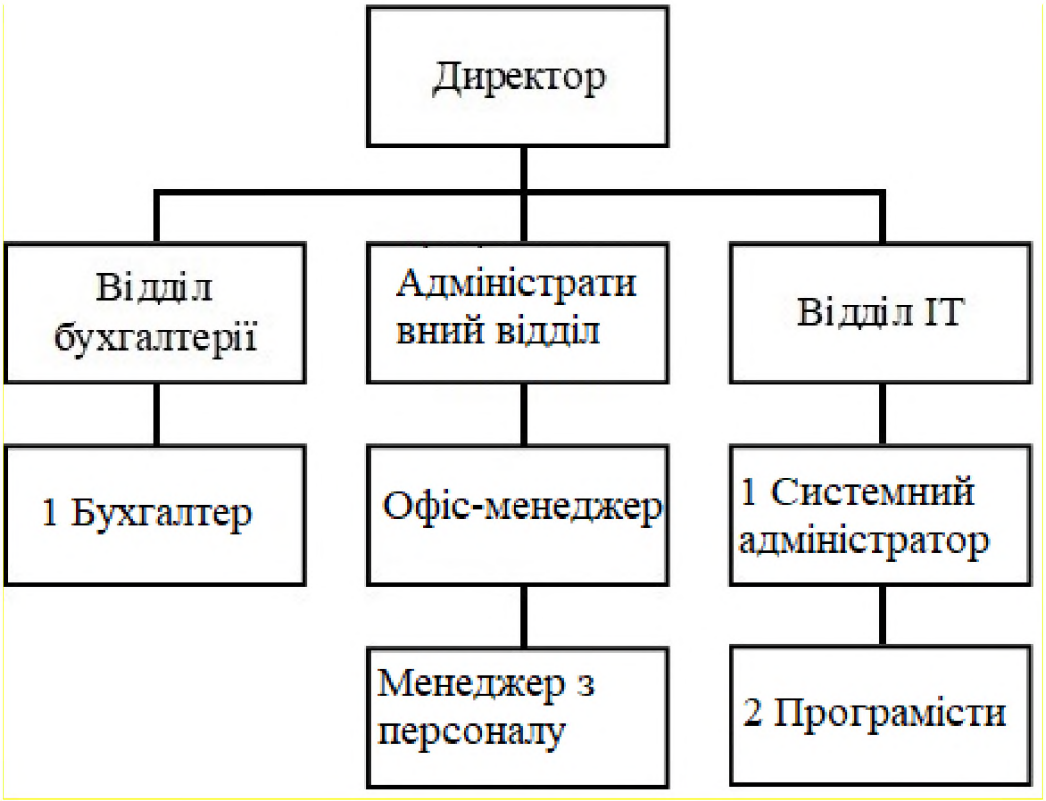

Рис. 2.1 – Організаційна структура підприємства ТОВ «ПФСОФТ»

ТОВ «ПФСОФТ» розташоване на 7 поверсі 9 – поверхового адміністративного будинку. Загальна площа приміщення, ке належить підприємству становить 90м 2. . Приміщення знаходиться у власності підприємства, про, що є відповідні записи в Державному реєстрі речових прав.

Територія будівлі впорядкована та асфальтована. Центральний вхід знаходиться зі західної сторони, запасні виходи знаходяться зі східної сторони. На всіх поверхах знаходяться офісні приміщення інших підприємств, які є власниками чи орендаторами.

Будівля оснащена металопластиковими вікнами з подвійним склопакетом. На центральному вході встановлені дві однакові металопластикові вхідні двері. Зі східної сторони будівлі розташоване місце паркування транспортних засобів.

Контрольована зона (КЗ) – обмежена периметром будівлі.

На центральному вході в будівлю встановлений КПП з постом цілодобової охорони. Охоронці на вахті – співробітники приватної охоронної фірми «Безпека», з якою у власника будівлі укладено договір надання послуг з цілодобової охорони будівлі. Охоронці працюють згідно зовнішніх організаційно-розпорядчих документів охоронної фірми, згідно договору. Приміщення будівлі обладнанні охоронною та пожежною системою сигналізації, яка підключена до ППКОП, який встановлений на КПП. Зовні будівля обладнана системою відеоспостереження, зображення виводиться на екран моніторів, які знаходяться на КПП охоронця. Відео з камер спостереження записується та зберігається на сервері охорони (S3), резервна копія відео-файлів резервуються двічі на день, кожні 12 годин на жорсткий диск HDD2, термін зберігання відео-файлів на сервері та жорсткому диску становить 30 днів.

На сьогоднішній день в офісі ТОВ «ПФСОФТ» не встановлено системи відеоспостереження. Системи контролю доступу на вхідних дверях не встановлено.

Відвідувачі, можуть зайти тільки за згодою директора ТОВ, який попередив офіс – менеджера.

Доступ електриків, техніків, сантехніків в офіс до комунікаційних систем надається за попередньою згодою з власником будівлі. Прибиральниця є фізичною – особою – підприємцем, з якою укладено договір на надання послуг. Прибиральниця виконує свою роботу в присутності співробітника компанії.

До будівлі підключені такі системи комунікації:

- система електропостачання підприємства підключена до міських електромереж, трьохфазним вводом на 10 кВ;

- система водопостачання, підключена до міської системи централізованого водопостачання підземними комунікаціями, пластиковими трубами.

- система каналізації, підключена до міської системи централізованого водовідведення підземними комунікаціями, пластиковими трубами.

- система мережі Інтернет підключена за допомогою оптично-волокнистого кабелю ТОВ «ТФСОФТ» має прямі договірні відносини з провайдером інтернету ТОВ «СТРІМ ЮКРЕЙН», ТОВ «ТЕЛЕМІСТ 2012» та працює згідно укладеного договору про надання телекомунікаційних послуг.

Канал зв'язку в межах корпоративної мережі забезпечується одним провайдером ТОВ «СТРІМ ЮКРЕЙН».

Персональні бази даних на паперових носіях знаходяться в сейфі, доступ та коди якого знаходяться у офіс–менеджера. А в електронному форматі на персональному комп'ютері у менеджера з персоналу та на сервері.

Інформація персональних баз даних підприємства зберігається у вигляді електронних документів, які створені за допомогою пакету прикладних програм Microsoft Office. Резервна копія документів зберігається на НЖМД, які в свою чергу знаходяться в сейфі.

Необхідна інформація друкується через принтер, що підключен до ПК менеджера з персоналу.

Паролі від облікових записів зберігаються у кожного користувача особисто. У пам'яті користувача, у вигляді записів на листку та у реєстрі Windows. Для кожного нового користувача, системним адміністратором створюється окремий обліковий запис, пароль від якого надається адміністратором. Виданий адміністратором пароль повинен бути змінений під час першої авторизації.

Правила розмежування доступу кожного користувача до окремого виду інформації, створюються та редагуються директором з системним адміністратором. У разі необхідності директор може запросити та переглянути будь-яку інформацію та документи компанії.

З огляду системи захисту, який наведено вище, можна зробити висновок: існуюча система захисту персональних даних на підприємстві ТОВ «ПФСОФТ» не забезпечує задовільного рівня захисту персональних даних.

2.2 Побудова системи захисту персональних даних для підприємства

2.2.1 Апаратне забезпечення системи захисту

Апаратні засоби захисту інформаційних систем - засоби захисту інформації та інформаційних систем, реалізованих на апаратному рівні. Ці інструменти є важливою частиною безпеки інформаційної системи, хоча розробники обладнання зазвичай залишають питання інформаційної безпеки програмістам.

У загальному вигляді інформаційну систему можна уявити як інформаційний простір і обслуговуючий його обчислювальний пристрій. Обчислення поділяються на окремі обчислювальні модулі, розташовані в інформаційному просторі. Схема реалізації обчислень може бути виражена так: обчислювальний пристрій отримує доступ до цього простору шляхом читання та редагування під керівництвом програми.

Для опису інформаційної системи введемо наступні поняття:

1. Вузол
2. Посилання
3. Контекст програми

Вузол - осередок даних довільного обсягу разом із посиланням на неї з обробного пристрою.

Посилання не тільки описують дані, але й містять усі права доступу до них. Система повинна контролювати те, що в операціях, які використовують посилання, не використовуються інші типи даних, а в операціях, які використовують параметри інших типів, посилання не можуть бути змінені.

Контекст програми - безліч всіх даних доступних для обчислень в конкретному модулі.

Апаратні засоби захисту інформаційної системи можуть включати в себе різні компоненти, такі як фізичні засоби захисту, криптографічні засоби захисту, системи автентифікації, системи контролю доступу та інші. Фізичні засоби захисту можуть включати в себе багато різних елементів, таких як замки, датчики вторгнення, камери спостереження та інші. Криптографічні засоби захисту використовуються для шифрування даних та забезпечення конфіденційності, цілісності та доступності інформації.

Системи автентифікації використовуються для ідентифікації користувачів та підтвердження їх прав доступу до інформації. Системи контролю доступу забезпечують контроль доступу до різних ресурсів системи, таких як файли, папки та програми.

Важливо пам'ятати, що захист інформаційної системи є постійним процесом, оскільки з часом з'являються нові загрози та вразливості. Тому виробники апаратури та програмного забезпечення повинні забезпечувати регулярні оновлення та патчі для своїх продуктів, а також встановлювати технічні засоби для виявлення та запобігання потенційним загрозам безпеки.

Для забезпечення безпеки інформаційної системи застосовуються різні засоби, включаючи апаратні. Апаратні засоби захисту можуть включати такі компоненти, як криптографічні модулі, біометричні системи і апаратні засоби контролю доступу.

Криптографічні модулі дозволяють зашифровувати дані, що передаються по мережі, тим самим забезпечуючи їх конфіденційність. Біометричні системи можуть використовуватися для ідентифікації користувачів, забезпечуючи доступ лише авторизованим особам. Апаратні засоби контролю доступу можуть бути встановлені на корпусі комп'ютера і забезпечувати доступ до системи лише з допомогою відповідного ключа або картки.

Окрім цього, апаратні засоби захисту можуть включати такі компоненти, як мережеві файрволи, системи виявлення вторгнень, мережеві контролери

безпеки та інші. Усі ці компоненти можуть допомогти забезпечити безпеку інформаційної системи на апаратному рівні, зменшуючи ризики інцидентів безпеки.

2.2.1.1. Захист на рівні біометричної аутентифікації.

Біометрична автентифікація є одним із засобів захисту персональних даних, оскільки вона використовує унікальні біологічні характеристики людини для ідентифікації особи. Однак, в той же час, вона може стати мішенню для кіберзлочинців, що прагнуть отримати доступ до цих даних.

Однією з основних проблем є збереження біометричних даних в безпеці. Це стає важливою задачею, оскільки, на відміну від паролів або пін-кодів, біометричні характеристики, такі як відбиток пальця, обличчя або голос, неможливо змінити після їх компрометації. Тому важливо застосовувати найкращі практики захисту даних, такі як шифрування, аутентифікація на рівні обладнання та захист від вторгнень.

Ще одна проблема полягає в тому, що біометричні дані можуть бути викрадені або підроблені. Наприклад, відбиток пальця може бути скопійований зі сканера, а обличчя може бути підроблене за допомогою фотографії. Це може бути покращено застосуванням додаткових технологій, таких як вимірювання живих показників, таких як пульс, температура тіла або поведінкові зміни, що зміцнюють процес біометричної автентифікації та зменшують ризик підробки.

Загалом, захист персональних даних на рівні біометричної автентифікації є складною задачею, яка вимагає поєднання кількох захисних методів та технологій.

Одним з найважливіших заходів захисту персональних даних на рівні біометричної автентифікації є забезпечення надійної захисту зберігання біометричних даних. Для цього можуть використовуватися такі методи, як шифрування даних та зберігання їх на безпечних серверах.

Окрім цього, важливо забезпечити захист від підробки біометричних даних. Для цього використовуються різні методи, такі як вимога до фізичної

присутності людини при реєстрації біометричних даних, використання мультифакторної автентифікації, застосування алгоритмів виявлення підробок тощо.

Також важливо забезпечити захист від недостовірної інформації, яка може бути отримана з біометричних даних. Наприклад, можливе отримання додаткової інформації про людину на основі її біометричних даних, таких як вік, стать, національність тощо. Тому важливо забезпечувати конфіденційність біометричних даних і не використовувати їх для інших цілей, крім автентифікації.

Таким чином, захист персональних даних на рівні біометричної автентифікації вимагає комплексного підходу, який включає в себе захист зберігання біометричних даних, захист від підробки та захист від недостовірної інформації, отриманої з цих даних. Тільки при такому підході можна забезпечити надійний захист персональних даних під час використання біометричної автентифікації.

Існує кілька методів біометричної автентифікації, які використовують різні фізіологічні або поведінкові риси особистості. Ось деякі з найбільш поширених методів:

1. Відбитки пальців: цей метод базується на унікальному рельєфі пальця кожної людини. Він використовується в багатьох системах безпеки, включаючи мобільні телефони та комп'ютери.

2. Розпізнавання обличчя: цей метод аналізує форму та розташування обличчя людини. Деякі системи використовують технологію розпізнавання 3D обличчя, щоб уникнути спроб обману, таких як використання фотографії.

3. Розпізнавання голосу: цей метод аналізує характеристики голосу, такі як тон, висота та мелодія голосу. Він використовується в банківських системах та інших системах безпеки, які потребують ідентифікації голосу.

4. Розпізнавання раковин вуха: цей метод використовує форму та структуру раковини вуха для ідентифікації особи. Він використовується в системах безпеки, що вимагають високої точності.

5. Розпізнавання DNA: цей метод використовує генетичні дані для ідентифікації особи. Він використовується в правоохоронних органах та медичних системах.

Нище наведена порівняльна таблиця (табл.. 2.1) вищевказаних методів розпізнавання особистості.

Таблиця 2.1 – Порівняння методів обмеження доступу до приміщення

	Опис	Переваги	Недоліки
Відбиток пальця	Аналіз унікальних характеристик відбитків пальців	Висока точність	Можливість пошкоджень шкіри пальців
Розпізнавання обличчя	Аналіз геометричних особливостей обличчя	Безконтактний, висока швидкість	Вплив освітлення, можливість спотворення
Сканування сітківки ока	Аналіз унікальних характеристик сітківки ока	Висока точність, мало впливає освітлення	Задоволення з ближніх відстаней
Сканування структури долоні	Аналіз геометричних та структурних особливостей долоні	Легкість застосування, висока точність	Залежність від стану шкіри, можливість спотворення
Голосовий аналіз	Аналіз голосу та його унікальних характеристик	Зручний, мало впливає фізичний стан користувача	Залежність від фонового шуму, можливість підробки
Розпізнавання DNA	Аналіз генетичної інформації, що міститься у ДНК	Висока точність, унікальність ідентифікатора	Складний процес збору та обробки зразків DNA, приватність

Розглянувши табл.. 2.1, можна зробити висновок стосовно доцільності використання різних методів біометричної автентифікації у різних умовах.

Таким чином, для підприємства ТОВ «ПФСОФТ» найбільш ефективним методом регулювання доступу до приміщень, які належать підприємству, буде комбінування двох різних засобів біометричної автентифікації: сканер відбитку пальця, встановлений на вхідних дверях в офіс, та доповнити цей метод системою розпізнавання обличчя, яке здійснюється за допомогою камери біля сканеру відбитку пальця.

Ця комбінація допоможе уникнути можливих проблем у разі пошкодження відбитків пальця у співпрацівників підприємства або у разі технічних труднощів з розпізнаванням обличчя.

Відбитки пальців та дані обличчя робітників підприємства попереднью (при прийомі на роботу) повинні бути від скановані та занесені у спеціалізовану базу даних, яка зберігається на сервері та доступ до якої обмежений директором підприємства та менеджером з персоналу.

2.2.1.2. Захист на рівні розширень Bios.

Захист ресурсів ПЕОМ на апаратному рівні може бути реалізований з використанням механізмів розширень Bios. У ПЕОМ, реалізованих на платформі Intel, первинна активізація обчислювальних ресурсів комп'ютера проводиться кодом процесора, що зберігається в основному у Bios. При включенні електроживлення код основного Bios «проектується» в область пам'яті F000 і управління передається на точку входу, визначену виробником Bios. Після цього код Bios проводить тестування обладнання, ініціалізацію векторів переривань, активізацію відеосистеми і деякі інші дії, що залежать від специфіки Bios. Код Bios містить типові процедури пошуку для так званих розширень Bios (Bios Extention). Розширення Bios – фрагменти коду, розроблені відповідно до наведених нижче правил, які (якщо їх дотримуються) контролюють передачі під час пошуку розширення. Розширення пошуку полягає у скануванні області пам’яті від C000 до F000 із кроком 512 байтів для

пошуку двобайтової сигнатури 55AA. Знайшовши цей підпис, проаналізуйте наступний (третій, починаючи з 55) байт, який представляє екстент Bios на 512-байтовій сторінці (або блоці).

Якщо вказане місце містить число, відмінне від 0, арифметична контрольна сума байтів обчислюється від довжини, зазначеної в 55-му байті до третього байта області пам'яті. Якщо ця сума збігається від 0 до четвертого (55 байт від першого) байта, керування передається. Якщо процедура RETF виникає в тілі коду, до якого передається керування (з урахуванням стану стека під час виклику розширення), то відбувається 43 повернення до основного Bios (тобто до процедури, яка шукає далі). для розширення). Тому існують механізми реалізації множинних функцій захисту на апаратному рівні ПК, тобто на «хронологічному» рівні на рівні завантаження операційної системи. Враховуючи те, що розширення Bios не може бути дуже великим, на цьому рівні можна реалізувати невелику кількість пов'язаних із безпекою функцій, а саме:

- ідентифікація та аутентифікація користувача (можливо, з використанням специфічного апаратного носія;

- заборона несанкціонованої завантаження ОС з обраних носіїв (наприклад з CD-ROM);

- контроль незмінності або цілісності апаратної або програмної компоненти ПЕОМ.

Треба звернути увагу, що перше розширення Bios, код якого буде виконано, це розширення VideoBios. Він розташований за адресою C000. Використовуючи дамп пам'яті, ви можете перевірити наявність наведених вище заголовків і команд. Програмування користувача просунутого Bios передбачає вирішення багатьох технічних завдань. Перший з них пов'язаний з тим, що програмування на мовах низького рівня в цьому випадку є вигідним. Друге пов'язане з тим фактом, що неможливо змінити стан програмної змінної, якщо вона не змінилася в PZP. Це вимагає належного перенесення коду в оперативну пам'ять за допомогою контрольних передач. Далі варто згадати, що під час

фази виконання коду Bios лише кілька службових функцій доступні для низькорівневого програмування - це служба клавіатури, відеослужба 10h interrupt і дискова служба 13h, реалізована в обробниках переривань 9h і 16h interrupt.

Також окремим завданням є правильне виконання фрагментів коду розширення. Як згадувалося вище, повернення до основного виконання Bios відбувається за допомогою команди RETF. Однак, якщо розширений виконуваний користувачем код 44 містить аварійний вихід (наприклад, у випадку неправильної автентифікації користувача), тоді апаратний перезапуск комп'ютера може бути використаний для примусової перерви у виконанні. Нарешті, про те, як реалізувати розширення Bios. В даний час існує велика кількість мережевих карт із розташуванням ПЗП або флеш-пам'яті, а також велика кількість захисних пристроїв (таких як плати ACORD), які пропонують можливість перепрограмування коду розширення Bios, де необхідний користувач може закласти механізми автентифікації (наприклад, як потрійний запит пароля).

Виходячи з вище написаного, можна запропонувати додаток до системи захисту наступним чином: BIOS підтримує метод завантаження з захищених пристроїв (оптичні диски, жорсткі диски, USB-носії тощо), що вимушує комп'ютер завантажувати операційну систему з конкретного носія, на якому вже завантажено необхідні автентифікаційні дані, без яких у прийнятний термін завантажити операційну систему неможливо.

Цю систему можна використовувати для доступу до ПЕОМ менеджеру з персоналу та/або інших посадових осіб, дані на ПЕОМ яких можуть потребувати додаткового рівня захисту. USB-ключі повинні зберігатися в сейфі в кабінеті директора.

2.2.1.3. Захист на рівні завантаження операційного середовища.

Локалізація механізмів захисту в структурах, пов'язаних з організацією початкового завантаження операційної системи, дозволяє вирішити багато важливих завдань комп'ютерної безпеки. Ці завдання пов'язані з «ранньої» ідентифікацією та аутентифікацією користувачів (при відсутності апаратного захисту), захистом від несанкціонованого завантаження операційної системи та отриманням спеціальних типів завантажувальних носіїв. Розглянемо ці питання докладніше.

Перша проблема – якщо наявна неможливість виконання процедур ідентифікації та верифікації (зокрема, процедур, зазначених у розширенні Bios) на етапі ініціалізації апаратних компонентів комп'ютера. Поєднання автентифікатора разом із завантажувачем дозволяє виконувати автентифікацію та автентифікацію на початку сеансу користувача.

Друге питання стосується захисту від завантаження неавторизованих копій операційної системи. Для вирішення цього завдання зазвичай використовуються прийоми обробки завантажень із зовнішніх носіїв або перетворення інформації на незнімний комп'ютерний носій (наприклад, зашифрований). У першому випадку завантаження із зовнішнього носія операційної системи практично неможливе, у другому – навіть при успішному завантаженні з неавторизованої копії операційної системи інформація буде недоступна.

Третя проблема пов'язана з формуванням завантажувальних носіїв (таких як дискети), які мають нестандартний вигляд для спеціального використання. Вирішення цих проблем зазвичай зводиться до програмування модифікованого завантажувача (або завантажувачів) для операційної системи.

Таким чином, очевидно, що для модифікації завантажувача необхідно в загальному випадку виконати наступні операції:

- замістити первинний код завантажувача власним фрагментом;

- зберегти вихідний код завантажувального сектора (в разі необхідності його виконання);

- з урахуванням необхідності розміщення первинного завантажника за тією ж адресою, що і модифікованого, забезпечити коректне переміщення модифікованого завантажувача в іншу область пам'яті без втрати управління.

Отже, необхідно розмістити змінений завантажувальний сектор замість основного (вихідного) завантажувача, а головний завантажувач (можливо, у перетвореному вигляді) у такому місці на дискеті чи жорсткому диску, щоб гарантовано гарантувалося збереження. . Для дискет рекомендується такий спосіб: повністю скопіювати нульову доріжку дискети на k-ту доріжку. Вихідна нульова доріжка заповнюється нулями (або іншим чином змінюється для отримання потрібного типу дискети). Встановіть необхідні програми замість завантажувального сектора. Запропонований спосіб дозволяє виключити використання гнучких дисків виробництва і не завантажувати з них. Доповнюючи DOS засобами перевірки цілісності, можна досягти відповідності всім вимогам ізоляції програмно-апаратного середовища.

Ввиходячи із проведеного аналізу апаратних засобів захисту інформації, було надано рекомендації щодо удосконалення системи захисту персональних даних, які матимуть позитивний вплив на захист інформації в цілому.

2.2.2 Програмне забезпечення системи захисту

Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та інші (рис. 2.2).

Рисунок 1.2 – Програмні засоби захисту інформації

Перевагами програмних засобів є універсальність, гнучкість, надійність, простота встановлення, можливості модифікації та розробки.

Мінуси – обмежені можливості мережі, використовує частину ресурсів файлового сервера та робочої станції, дуже чутливий до випадкових або навмисних змін, може залежати від типу комп'ютера (його апаратного забезпечення).

2.2.2.1. Антивірусні програми.

Антивірусна програма (антивірус) - програма для виявлення комп'ютерних вірусів і лікування інфікованих файлів, а також для профілактики - запобігання зараженню файлів або операційної системи шкідливим кодом. Для захисту від вірусів використовують три групи методів:

1.1. Методи, засновані на аналізі вмісту файлів: метод сканування сигнатур, перевірка цілісності і сканування підозрілих команд.

1.2. Методи, засновані на відстежуванні поведінки програм при їх виконанні.

1.3. Методи регламентації порядку роботи з файлами і програмами. Ці методи відносяться до адміністративних заходів забезпечення безпеки.

Метод сканування сигнатур (сигнатурний аналіз, сигнатурний метод) заснований на пошуку в файлах унікальною послідовності байтів - сигнатури, характерної для певного вірусу. Перевагою цього методу є відносно низький рівень помилкових спрацьовувань, а основним недоліком є те, що неможливо виявити нові віруси в системі, яка не має сигнатури в базі даних антивірусної програми.

Метод контролю цілісності ґрунтується на тому, що будь-які несподівані та незрозумілі зміни даних на диску є підозрілими подіями, які потребують особливої уваги з боку антивірусних систем. Віруси обов'язково залишають сліди свого існування (зміна даних існуючих (особливо системних або виконуваних) файлів, 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.

Метод сканування підозрілих команд (евристичний сканування, евристичний метод) заснований на виявленні певної кількості підозрілих команд та/або скануванні файлів на ознаки підозрілих кодових послідовностей (наприклад, команда форматування жорсткого диска або введення запущений процес або функції у виконуваному коді).

Метод відстеження поведінки програм принципово відрізняється від методів сканування вмісту файлів, згаданих раніше. Цей метод заснований на аналізі поведінки запущених програм, який можна порівняти з затриманням злочинця «за руку» на місці злочину.

При використанні антивірусних систем, які аналізують поведінку програм, завжди існує ризик виконання команд вірусного коду, які можуть пошкодити захищений комп'ютер або мережу. Для усунення подібних недоліків пізніше були розроблені методи емуляції (імітації), які дозволяють запускати тестову програму в штучно створеному (віртуальному) середовищі (часто її називають пісочницею) без ризику руйнування інформаційного середовища. Методи аналізу поведінки програм показали свою ефективність у виявленні як відомих, так і невідомих шкідливих програм.

Наразі існує декілька найбільш розповсюджених антивірусних програм, порівняння яких наведено у таблиці нижче. У табл. 2.2-2.3 наведено порівняння методів роботи цих програм.

Таблиця 2.2 – Порівняння антивірусних программ

	Основні функції	Методи роботи	Операційні системи
Norton Antivirus	Сканування на віруси, блокування загроз, фаєрвол	Підписи, евристичний аналіз, хмарні технології	Windows, Mac

	Основні функції	Методи роботи	Операційні системи
McAfee Antivirus	Антивірусний захист, фаєрвол	Підписи, евристичний аналіз	Windows, Mac, Android, iOS
Avast Antivirus	Сканування на віруси, блокування загроз, фаєрвол	Підписи, евристичний аналіз, поведінковий аналіз	Windows, Mac, Android, iOS
Zillya	Виявлення та блокування, Сканування на віруси	Підписи, евристичний аналіз, поведінковий аналіз, Сигнатурний аналіз	Windows
Bitdefender Antivirus	Сканування на віруси, блокування загроз, фаєрвол	Підписи, евристичний аналіз	Windows, Mac, Android, iOS
Avira Antivirus	Сканування на віруси, блокування загроз	Підписи, евристичний аналіз, хмарні технології	Windows, Mac, Android, iOS
ESET NOD32 Antivirus	Сканування на віруси, блокування загроз, фаєрвол	Підписи, евристичний аналіз	Windows, Mac, Android
AVG Antivirus	Сканування на віруси, блокування загроз, фаєрвол	Підписи, евристичний аналіз, поведінковий аналіз	Windows, Mac, Android

Таблиця 2.3 – Порівняння методів роботи антивірусів

	Сильні сторони	Слабкі сторони
Аналіз вмісту файлів	- Ефективний у виявленні відомих вірусів та шкідливих програм - Швидкий процес сканування	- Менш ефективний у виявленні нових, невідомих вірусів - Може спричинити помилкові спрацювання при спільному використанні
Методи, засновані на відстежуванні поведінки програм при їх виконанні	- Здатність виявляти нові, невідомі віруси - Здатність виявляти зміну поведінки шкідливих програм	- Можливість помилкових спрацювань, особливо при роботі з легітимними програмами
Методи регламентації порядку роботи з файлами і програмами	- Забезпечення контролю над діями файлів та програм - Виявлення підозрілих або небезпечних дій	- Обмежена ефективність у виявленні нових, невідомих вірусів
Метод сканування сигнатур	- Висока ефективність у виявленні відомих вірусів та шкідливих програм - Швидкий процес сканування	- Менш ефективний у виявленні нових, невідомих вірусів - Вимагає постійного оновлення бази сигнатур
Метод контролю цілісності	- Виявлення змін у програмах та системних файлів, що може свідчити про втручання вірусів	- Менш ефективний у виявленні нових, невідомих вірусів - Вимагає встановлення спеціальних програм
Метод сканування підозрілих команд	- Здатність виявляти та блокувати шкідливі команди, що виконуються в системі	- Можливість помилкових спрацювань та блокування легітимних команд
Метод відстеження поведінки програм	- Здатність виявляти нові, невідомі віруси та шкідливі програми - Виявлення підозрілих дій	- Вимагає великої кількості обчислювальних ресурсів - Можливість помилкових спрацювань

Спеціалізовані програмні засоби захисту інформації від несанкціонованого доступу володіють в цілому кращими можливостями і характеристиками, ніж вбудовані засоби. Крім програм шифрування і криптографічних систем, існує багато інших доступних зовнішніх засобів захисту інформації.

Як можна побачити з таблиць 2.2 та 2.3 усі представлені антивіруси використовують один принцип визначення вірусів та іншого шкідливого програмного забезпечення, тому серед наведених програм виділяється програма Avast, оскільки вона використовує додатковий метод виявлення шкідливого програмного забезпечення – поведінковий аналіз. Однак у 2020 році вокруг компанії, яка володіє антивірусом, виник гучний скандал [13] щодо використовування персональних даних та неетичних методів ведення бізнесу, що ставить під сумнів його ефективність та доцільність використання. Тому треба звернути увагу на інші досить популярних та ефективних антивіруси - McAfee Antivirus та Norton Antivirus (рис. 2.3).

Рис. 2.3 - Інтерфейс програми Norton

2.2.2.2. Міжмережеві екрани.

Міжмережеві екрани (також звані брандмауерами або firewall). Між локальної та глобальної мережами створюються спеціальні проміжні сервери, які інспектують і фільтрують весь трафік мережевого і транспортного рівнів. Це дозволяє різко знизити загрозу несанкціонованого доступу ззовні в корпоративні мережі, але не усуває цю небезпеку повністю. Більш захищена різновид методу - це спосіб маскараду (masquerading), коли весь вихідний з локальної мережі трафік посилається від імені firewall-сервера, роблячи локальну мережу практично невидимою.

В табл.. 2.4 наведено порівняння найбільш розповсюджених міжмережевих екранів.

Таблиця 2.4 – Порівняння міжмережевих екранів

	Опис	Функціональні можливості	Додаткові функції	Вартість (платна/ ні)
Cisco ASA	Хорошо відомий інтегрований міжмережевий екран, який надає функціональні можливості для захисту мережі та розширених функцій маршрутизації.	Фільтрація пакетів, VPN, NAT, SPI, IDS/IPS	Захист від DDoS, контроль пропускної здатності, QoS	Платна
Fortinet FortiGate	Інтегрований мережевий пристрій, який комбінує міжмережевий екран з функціями UTM (Unified Threat Management) та веб-фільтрації.	Фільтрація пакетів, VPN, NAT, SPI, IDS/IPS, UTM	Веб-фільтрація, захист від витоку даних, аналітика трафіку	Платна

	Опис	Функціональні можливості	Додаткові функції	Вартість (платна/ ні)
Palo Alto Networks	Міжмережевий екран, який забезпечує апаратний та програмний захист мережі шляхом комбінації міжмережевого екрана, IDS/IPS та системи управління безпекою.	Фільтрація пакетів, VPN, NAT, SPI, IDS/IPS	Аналіз SSL-трафіку, захист від загроз за допомогою штучного інтелекту	Платна
Check Point Firewall	Міжмережевий екран з інтегрованими функціями захисту мережі, такими як VPN, захист від загроз та фільтрація пакетів.	Фільтрація пакетів, VPN, NAT, SPI, IDS/IPS	Захист від атаки постачальника, управління політиками безпеки	Платна
Juniper Networks SRX	Мережевий пристрій, що комбінує міжмережевий екран з маршрутизацією та комутацією для надання широкого спектру функціональності захисту мережі.	Фільтрація пакетів, VPN, NAT, SPI, IDS/IPS	Автоматична корекція загроз, прискорена комутація, віртуалізація	Платна
pfSense	Відкрите програмне забезпечення, яке надає міжмережевий екран, побудований на основі FreeBSD. Відмінно підходить для домашнього використання та невеликих бізнес-мереж.	Фільтрація пакетів, VPN, NAT, SPI, IDS/IPS	Веб-кешування, віртуалізація, підтримка розширень	Безкоштовна

Серед наведених у табл.. 2.4 файрволів треба виділити pfSense через відкритий код, що дозволяє провести незалежний аудит цього програмного забезпечення та/або, у разі необхідності, написати додаткові модулі до

програмного забезпечення. Окрім цього, досить оптимальним варіантом може бути продукт Fortinet FortiGate, який забезпечує захист від витоку даних та відстеження трафіку.

2.2.2.3. Проксі сервера та віртуальні приватні мережі.

Proxy-servers. Весь мережевий/транспортний трафік між локальними та глобальними мережами повністю заборонений - маршрутизації як такої немає, а запити з локальної мережі до глобальної проходять через спеціальні проксі-сервери. Зрозуміло, що в цьому випадку запити з глобальної мережі в локальну стають практично неможливими. Цей метод не забезпечує достатнього захисту від атак на більш високих рівнях - наприклад, на рівні длдатку.

VPN (віртуальна приватна мережа) дозволяє передавати секретну інформацію через мережі, в яких можливе прослуховування трафіку сторонніми людьми. Використовувані технології: PPTP, PPPoE, IPSec.

В табл.. 2.5 наведено порівняння VPN-сервісів.

Таблиця 2.5 – Порівняння VPN-сервісів

	Відсоток зменшення швидкості загрузки	Відсоток зменшення швидкості вигрузки	Відсоток збільшення часу затримки
ExpressVPN	10% або менше	10% або менше	0-5%
NordVPN	10% або менше	10% або менше	0-5%
Surfshark	10% або менше	10% або менше	0-5%
Private Internet Access (PIA)	10% або менше	10% або менше	0-5%
CyberGhost	20-30%	20-30%	5-10%
VyprVPN	30-40%	30-40%	10-15%
IPVanish	40-50%	40-50%	15-20%
Hotspot Shield	50% або більше	50% або більше	20% або більше

Виходячи із змісту табл.. 2.5 серед антивірусних програм треба знайти компроміс серед швидкістю роботи та ефективністю захисту мережі, і використання різних сервісів може відповідати різним умовам – так, сервіс Hotspot Shield забезпечує високий рівень захисту від прослуховування та витоку інформації з приватної мережі, але сильно обмежує швидкість роботи. Одними з найбільш популярних сервісів є сервіси Nord та Express через наявний достатній функціонал, та досить високу швидкість роботи.

2.2.2.4. Програми для запобігання несанкціонованого доступу до даних.

Програми для запобігання несанкціонованому доступу до конфіденційної інформації умовно можна розділити на три типи:

1. програми для шифрування інформації;
2. програми, що приховують інформацію;
3. програми, які не шифрувальні інформацію, але блокують несанкціонований доступ або обмежують доступ до даних.

На практиці багато програм можуть обробляти різні типи одночасно. Наприклад, деякі програми, які не шифрують інформацію, але блокують несанкціонований доступ до неї, також можуть приховувати цю інформацію на жорсткому диску, щоб відповідні файли або папки не відображалися в провіднику.

Програми для шифрування даних можна умовно розділити на два типи:

1. Симетричне шифрування. У цьому методі для шифрування і розшифрування використовується один і той же ключ. Такий метод дозволяє ефективно захистити інформацію від несанкціонованого доступу, але ключ також потрібно захистити, оскільки з його допомогою можна розшифрувати дані.

2. Асиметричне шифрування. У цьому методі для шифрування і розшифрування використовуються два різних ключі - приватний і публічний. Публічний ключ можна розголошувати широкій аудиторії, а приватний ключ залишається тільки у власника інформації. Зашифровану інформацію можна розшифрувати тільки з допомогою приватного ключа, який захищений від несанкціонованого доступу.

Програми для шифрування даних допомагають забезпечити конфіденційність інформації, що передається через мережу Інтернет або зберігається на комп'ютері. Важливо вибрати правильний метод шифрування в залежності від ваших потреб та рівня безпеки, який потрібно забезпечити. Відкритий і секретний ключі утворюють унікальну пару і пов'язані один з одним математично. Ідея полягає в тому, що, знаючи відкритий ключ, принципово неможливо обчислити секретний ключ.

Як правило, програми, які реалізують асиметричне шифрування на основі пари ключів, використовуються не для зберігання інформації, а для безпечної передачі даних через Інтернет. Наприклад, якщо потрібно надіслати інформацію в зашифрованому вигляді, можливо згенерувати пару ключів і надіслати відкритий ключ своєму кореспонденту. Сторона, яка спілкується, шифрує інформацію за допомогою вашого відкритого ключа та надсилає її вам. Цю зашифровану інформацію можна розшифрувати лише за допомогою закритого ключа, який зберігається у вас і поєднується з відкритим ключем, який використовується для шифрування інформації. Якщо інформація шифрується лише для безпечного зберігання, то для симетричного шифрування даних краще використовувати один ключ. Слід зазначити, що деякі програми дозволяють генерувати ключі шифрування та зберігати їх пізніше. Крім того, припустимо, що ключ зберігатиметься на зовнішньому носії, наприклад, флеш-пам’яті USB.

В табл.. 2.6 наведено порівняння програм шифрування даних.

Таблиця 2.6 – Порівняння програм шифрування даних

	Тип шифрування	Алгоритм шифрування	Розрядність ключів	ОС	Простота використання	Вартість
VeraCrypt	Диск и файлове шифрування	AES, Serpent, Twofish	256 біт	Windows, Mac, Linux	Складне	Безкоштовно
BitLocker	Диск и файлове шифрування	AES	128 або 256 біт	Windows	Просте	Безкоштовно
AxCrypt	Файлове шифрування	AES	128 або 256 біт	Windows	Просте	Безкоштовно (з обмеженнями) Платне
GPG Suite	Файлове шифрування й електронний підпис	RSA, AES, OpenPGP	Різні розміри	Mac	Складне	Безкоштовно
7-Zip	Файлове шифрування	AES	256 біт	Windows, Mac, Linux	Просте	Безкоштовно

Серед наведених у табл.. 2.6 програм для шифрування даних треба звернути увагу на програму VeraCrypt (рис. 2.4), яка є інструментом з відкритим кодом, який виник на основі припинившого свою роботу TrueCrypt, що зарекомендував себе як ефективна та досить многофункціональна програма захисту даних – в тому числі і персональних. Так, у 2015 р. було проведено аудит програми TrueCtypt [14], який не виявив серйозних уразливостей у цій програмі.

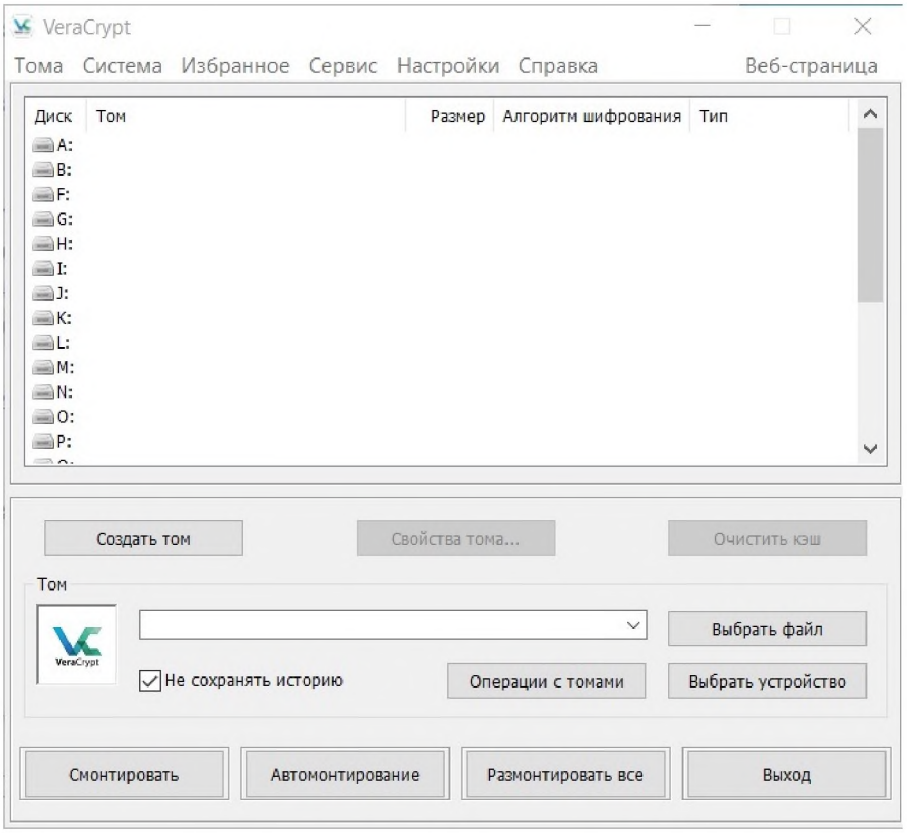

Рисунок 2.4 – Інтерфейс програми VeraCrypt

Довжина ключа в багатьох алгоритмах шифрування становить 256 біт, навіть якщо він записаний у шістнадцятковому форматі. Якщо ключ не потрібно зберігати окремо, ви можете встановити для нього парольну фразу. Сам пароль не є ключем шифрування, але за допомогою спеціального алгоритму хешування пароль завжди можна перетворити на потрібний ключ. Хешування або пошук Хеш-функції — це математичний односторонній процес, який використовується для перетворення пароля в набор бітів фіксованої довжини. Знання хеш-функції пароля взагалі унеможливлює розрахунок пароля - ось що означає одностороннє перетворення.

Таблиця 2.7 – Порівняння алгоритмів хешування даних

Метод	Опис	Властивості	Приклади
MD5	Використовується для обчислення 128-бітного хешу	Швидкий, використовується для перевірки цілісності даних	md5sum, hashlib.md5 (Python)
SHA-1	Використовується для обчислення 160-бітного хешу	Застарілий, використовується рідко через вразливості	hashlib.sha1 (Python)
SHA-256	Використовується для обчислення 256-бітного хешу	Безпечний, широко використовується для захисту даних	hashlib.sha256 (Python), SHA-256 (Bitcoin)
SHA-3	Використовується для обчислення хешу різної довжини (наприклад, 224, 256 біт)	Безпечний, заміна SHA-2	hashlib.sha3_256 (Python)
BLAKE2	Використовується для обчислення хешу різної довжини (наприклад, 256, 512 біт)	Швидкий, міцний криптографічний захист	hashlib.blake2s (Python)
Whirlpool	Використовується для обчислення 512-бітного хешу	Висока стійкість до зламу, використовується в деяких криптографічних протоколах	hash-whirlpool (PHP), pycrypto (Python)

Хешування даних дозволяє не тільки ефективно перевіряти цілісність передаваємих даних, але й, як було зазначено вище, ще займають важливе місце в алгоритмах шифрування даних, генеруючи ключі шифрування та дешифрування з заданих паролей. Одним з найбільш використовуваних алгоритмів хешування є алгоритм SHA-3, який вже показав себе як ефективний

та надійний алгоритм хешування. Саме за допомогою цього алгоритму має сенс створення системи електронного підпису на документах, які містять персональні дані, що дозволить відстежити несанкціоноване втручання.

Існує багато різних алгоритмів шифрування, і багато програм дозволяють вибрати алгоритм шифрування. В даний час найбільш популярним є алгоритм шифрування AES з довжиною ключа 256 біт. В принципі, підтримку програмою багатьох алгоритмів шифрування навряд чи можна зарахувати до її сильних сторін. Досить, щоб програма підтримувала тільки один алгоритм шифрування, стійкий до пароля, наприклад, AES з довжиною ключа 256 біт. Розкрити такий шифр неможливо, тобто ключ до нього не знайти. Насправді, якщо довжина ключа становить 256 біт, загалом існує 2256 = 1,15792 • 10^77 різних комбінацій ключів. Якщо ми використовуємо підхід сортування ключів і припустимо для простоти, що комп'ютер здатний сортувати мільйон ключів за секунду (хоча фактична швидкість ключів сортування сучасних комп'ютерів набагато нижча), для сортування всіх знадобиться 3,78 • 10^63 років. ключі. Тому сучасні методи шифрування забезпечують досить надійний захист даних.

Програми, що приховують дані. Програми для приховування даних просто приховують дані на вашому комп'ютері, щоб їх неможливо виявити традиційними методами доступу. Доступ до даних можливий тільки при запуску спеціальної утиліти, але для цього потрібно знати пароль.

Програми, які блокують або обмежують доступ до даних. Деякі програми дозволяють заборонити доступ до інформації без шифрування самих даних. Тобто припустимо, що вам потрібно знати пароль для доступу до даних (відкрити файл). Крім того, такі програми часто не тільки блокують доступ до даних, а й обмежують доступ до даних. Наприклад, вони дозволяють встановити режим доступу «тільки для читання», тобто такий, який не має дозволу на зміну документа тощо. Плюси і мінуси різних варіантів. Програми, які блокують або обмежують доступ до даних, а також програми, які приховують інформацію, не можна вважати повністю надійними. При цьому вони дозволяють дуже швидко обробляти дані, що є їх незаперечною

перевагою. Програма, що використовує парольний захист, тобто шифрування даних, забезпечує високу надійність, але процес шифрування і дешифрування вимагає часу, а швидкість виконання залежить від обчислювальної потужності комп'ютера.

Отже, виходячи з проведеного аналізу програмних методів захисту інформації, який було здійснено вище, персональні дані, які зберігаються на ПЕОМ менеджера з персоналу та на сервері, потребують захисту за допомогою шифрування – найбільш оптимальною програмою для забезпечення захисту персональних даних є програма VeraCrypt, яка вже зарекомендувала себе, як надійна та ефективна система захисту інформації. Також, через вимушений перехід до дистанційної форми роботи, для забезпечення захисту від витоку інформації найбільш доцільним буде застосування VPN-сервісу NordVPN або ExpresVPN, які забезпечують високий рівень захисту при досить малому впливу на продуктивність. Також для контролю цілісності даних треба використовувати програму для створення електронного підпису – DocuSign.

2.2.3 Організаційне забезпечення системи захисту

Згідно з ДСТУ 3396.1-96 [15] «Організаційні заходи захисту інформації — комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціювання засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення ТЗІ».

Аудит існуючих систем захисту персональних даних – це дослідження різних процесів обробки персональних даних. А також аналізує документи, що стосуються організаційно-адміністративного напряму діяльності компанії, різноманітні пропозиції, вдосконалення існуючих систем тощо. Аудит захисту персональних даних також може включати моніторинг існуючих систем у разі зміни законодавства або будь-яких загроз. Крім того, це можуть бути технічні заходи щодо створення системи захисту персональних даних.

Аудит існуючих систем захисту персональних даних – це дослідження різних процесів обробки персональних даних. А також аналізує документи, що стосуються організаційно-адміністративного напряму діяльності компанії, різноманітні пропозиції, вдосконалення існуючих систем тощо. Аудит захисту персональних даних також може включати моніторинг існуючих систем у разі зміни законодавства або будь-яких загроз. Крім того, це можуть бути технічні заходи щодо створення системи захисту персональних даних.

Важливо розуміти, для чого потрібно вживати заходів щодо захисту персональних даних. Якщо перевіряється документація, навіть частина інформаційної системи персональних даних не відповідають вимогам законодавства, то це послужить причиною того, що виникне відповідальність за порушення вимог щодо захисту персональних даних.

Наразі в процесі обробки персональних даних вирішені відповідні питання, такі як стандартизація процесу збору персональних даних та забезпечення інформаційної безпеки, про що добре відомо більшості юристів. Зрозуміло, що законодавство ще не завершене та потребує доопрацювання, але основні положення регулює Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010[1]. Отже, відповідно до ст. Стаття 12 вищезазначеного закону визначає, що збір персональних даних є частиною їх обробки, яка передбачає відбір або систематизацію інформації про фізичних осіб.

Суб’єкт персональних даних інформується про володільця персональних даних, склад і зміст зібраних персональних даних, права, передбачені законом, мету збирання персональних даних та особу, якій надаються його персональні дані. передано: під час збору персональних даних, якщо вони збираються з персональних даних суб’єкта, в інших випадках – протягом тридцяти робочих днів з дати збору персональних даних.

Окрім вищезазначених законів, юридичні та фізичні особи мають можливість використовувати для вирішення питань, пов’язаних із забезпеченням власної інформаційної безпеки, положення Цивільного кодексу

України, Закону України «Про інформацію» та інших актів законодавства України. З огляду на майбутні кроки України та євроінтеграційні амбіції, менш вивченим, але більш цікавим питанням є ознайомлення, дослідження та аналіз нормативних актів щодо захисту персональних даних, особливо щодо збору в країнах ЄС.

Питання захисту персональних даних та інформаційної безпеки в Інтернеті на даний момент є найбільш актуальним і активно розвивається. У результаті 25 травня 2018 року набули чинності нові правила захисту персональних даних в Інтернеті для користувачів, які знаходяться в Європейській економічній зоні (ЄЕЗ). Тут слід розуміти, що до ЄЕЗ входять не лише країни самого Європейського Союзу, а й країни Європейської асоціації вільної торгівлі (ЄАВТ), крім Швейцарії. Угода про створення Європейської економічної зони була підписана в 1992 році і набула чинності 1 січня 1994 року. ЄЕЗ базується на тих же «чотирьох свободах», що й Європейське співтовариство: вільний рух товарів, людей, послуг і капіталу між країнами ЄЕЗ. Тому існує режим вільної торгівлі між країнами ЄАВТ, які є членами ЄЕЗ та ЄС. Це дозволяє таким країнам ЄАВТ, як Ісландія, Норвегія та Ліхтенштейн, брати участь у єдиному європейському ринку без приєднання до ЄС. Відповідно до Угоди про Європейський економічний простір, розширення ЄС тягне за собою розширення Європейського економічного простору. Тому зараз Європейський економічний простір охоплює 30 країн.

Майже всі великі інтернет-компанії, включаючи Google, Facebook та Twitter, підпадають під дію GDPR. У цілях GDPR - забезпечити ще більший захист персональних даних людини, включаючи, але не обмежуючись, її релігійні чи політичні переконання. Штрафи за недотримання правил є значними: до 20 мільйонів євро або 4% від загального обороту за порушення. Крім того, GDPR надає користувачам можливість компенсувати будь-яке суттєве та / або нематеріальне порушення GDPR. GDPR застосовується до даних, які збираються, обробляються та / або зберігаються в Європі, незалежно від того, де дані збираються. Якщо, наприклад, фізична особа має в Україні

інтернет-магазин з інформаційним бюлетенем і на нього підписався принаймні один потенційний клієнт з Європейського Союзу, то такий інтернет-магазин підпорядковується правилам GDPR, що відкриває нові можливості для юристів покращити свої знання та надати допомогу клієнтам.

Важливою умовою GDPR є те, що з моменту набрання чинності цим законом передача даних за межі ЄС до будь-якої країни, яку ЄС вважає несумісною з вимогами законодавства про захист персональних даних, забороняється. дані передаються за межі ЄС для обробки або зберігання за явною згодою користувача, який володіє даними. У будь-якій ситуації, коли ви запитуєте дані користувача, спочатку запитайте себе: як це вплине на права власника даних? GDPR визначає наступні юридичні права, які мають власники даних: право на доступ, право на заперечення, право на інформацію, право на виправлення, право на передачу даних, право на видалення, право не підлягати автоматичному прийняттю рішень, право на обмежити обробку даних. Однак власники даних також мають права. Наприклад, якщо користувач підписався на вашу розсилку. З часом він вирішив, що більше не хоче отримувати розсилку, і скасував підписку. У цьому випадку ви можете просто назавжди видалити електронну адресу користувача. Однак, коли користувачі підписуються на інформаційний бюлетень, вам потрібно знати їхню IP-адресу, щоб відповідати їхній згоді на отримання інформаційного бюлетеня (і ви повинні), оскільки ви маєте право зберігати ці дані, щоб підтвердити, що ваш сайт відповідає GDPR.

Оператор до початку обробки персональних даних зобов'язаний повідомити уповноважений орган із захисту прав суб'єктів персональних даних про свій намір здійснювати обробку персональних даних, за винятком таких випадків:

1) відносяться до суб'єктів персональних даних, яких пов'язують з оператором трудові відносини;

2) отриманих оператором у зв'язку з укладенням договору, стороною якого є суб'єкт персональних даних, якщо персональні дані не поширюються, а також не надаються третім особам без згоди суб'єкта персональних даних і

використовуються оператором виключно для виконання зазначеного договору та укладення договорів з суб'єктом персональних даних;

3) що відносяться до членів (учасників) громадського об'єднання чи релігійної організації та оброблюваних відповідними громадським об'єднанням або релігійною організацією, для досягнення законних цілей, передбачених їх установчими документами, за умови, що персональні дані не будуть поширюватися без згоди в письмовій формі суб'єктів персональних даних;

4) є загальнодоступними персональними даними;

5) включають в себе тільки прізвища, імена та по батькові суб'єктів персональних даних;

6) необхідних з метою одноразового пропуску суб'єкта персональних даних на територію, на якій знаходиться оператор, або в інших аналогічних цілях;

Етап обстеження інформаційних систем персональних даних

На етапі обстеження інформаційних систем персональних даних (ПД) проводяться ряд робіт для визначення стану систем та встановлення необхідних заходів для їх захисту. Дані роботи включають наступні етапи:

1. Формування переліку ПД, інформаційних систем і технічних засобів:

На цьому етапі складається перелік всіх персональних даних, які обробляються в організації, а також перелік інформаційних систем та технічних засобів, які використовуються для обробки цих даних.

2. Визначення підрозділів і працівників, які обробляють ПД:

На цьому етапі встановлюється, які підрозділи та працівники мають доступ до персональних даних і займаються їх обробкою. Це допомагає визначити потенційні точки доступу до інформації і встановити контроль над ними.

3. Визначення категорій ПД:

Проводиться класифікація персональних даних на різні категорії в залежності від їх особливостей і рівня конфіденційності. Наприклад, це можуть бути особисті дані клієнтів, медичні записи або фінансова інформація.

4. Розробка опису об'єкта захисту:

Створюється детальний опис інформаційних систем та технічних засобів, які використовуються для обробки ПД. Опис включає склад і характеристики цих засобів, а також їх функції та роль у захисті інформації.

5. Класифікація інформаційних систем ПД:

Здійснюється попередня класифікація інформаційних систем, які обробляють ПД, на основі їх характеристик та рівня конфіденційності. Це допомагає встановити вимоги щодо безпеки для кожної системи окремо.

6. Оцінка заходів і витрат на приведення систем у відповідність:

На цьому етапі проводиться оцінка необхідних заходів і витрат для приведення інформаційних систем ПД у відповідність з вимогами безпеки. Враховуються технологічні, організаційні і фінансові аспекти для реалізації необхідних змін і покращень.

Результатом робіт на етапі обстеження є набір документів і висновків, включаючи:

- перелік пд і категорій пд;
- перелік інформаційних систем та технічних засобів, що використовуються для обробки пд, та аналіз їх стану;
- засоби захисту пд, які вже використовуються;
- перелік підрозділів та співробітників, які обробляють пд;
- класифікація інформаційних систем, що обробляють пд, на типові спеціальні категорії;
- акти класифікації інформаційних систем, що обробляють пд;
- опис об'єктів захисту;
- уточнення загроз та вимог до систем захисту пд;
- перелік необхідних заходів та орієнтовна вартість робіт для приведення інформаційних систем пд у відповідність з вимогами.

Додатково, важливо провести оцінку можливості дезідентифікації або зниження класифікації інформаційних систем та необхідні роботи для досягнення вимог безпеки

Що стосується сфери інформаційної безпеки адміністративних органів, то її зазвичай поділяють на: фізичний рівень, рівень програмного забезпечення, технічний рівень, адміністративний рівень, технічний рівень, рівень користувача, рівень мережі та рівень програми. Давайте детальніше розглянемо кожен із цих рівнів. 1. Фізичний рівень - організація та фізичний захист інформаційних ресурсів, використовувані інформаційні технології та технології управління.

1. Програмно-технічний рівень - здійснюється ідентифікації і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

2. Управлінський рівень - здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки органів виконавчої влади.

3. Технологічний рівень - здійснюється реалізації політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

4. На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на центральні та місцеві органи виконавчої влади, унеможливлення інформаційного впливу з боку соціального середовища.

5. На сітьовому рівні дана політика реалізується у форматі координації дій органів виконавчої влади, які пов'язані між собою однією метою.

6. Процедурний рівень - вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

В рамках ОЗІБ здійснюється організаційна діяльність із специфікації, технології програмного забезпечення, фізики та інших напрямків забезпечення ІС, регламентується процес функціонування інформаційної системи,

використання інформаційних ресурсів, діяльність обслуговуючого персоналу ІС та загального підприємства. співробітників Взаємодія користувача з системою Замовлення. Під організаційною діяльністю розуміється діяльність, яка використовує планування, керівництво, координацію, контроль, прийняття управлінських рішень, надання допомоги, забезпечення виконання завдань вчасно та сприяння виконанню пов'язаних заходів у вищезазначених напрямках. Загалом ОЗІБ виконує наступні функції: інформаційну (збирати, обробляти та використовувати всі доступні види інформації, які впливають на досягнення цілей організації), міжособистісну (забезпечувати взаємодію між керівництвом, працівниками, зовнішніми організаціями, споживачами та всіма зацікавленими сторонами), прийняття рішень. (вибір найкращого рішення, вирішення конфліктів, запобігання виникненню проблем). Розглянемо різні наукові підходи до визначення структури ОЗІБ. Відповідно до процесного підходу ОЗІБ можна розглядати як замкнутий процес управління і представити у вигляді моделі «Плануй-Виконуй-Перевіряй-Дій» («Plan-Do-CheckAct»).

Компоненти системи підтримки ІБ відповідно до системного підходу поділяються на три групи: основа (включаючи: основу, структуру, заходи, інструменти), напрямок (їхнє призначення: захистити об'єкти, процеси та канали зв'язку ІБ, керувати та контроль системи ІБ), фази (як це працює: ідентифікація ключових ресурсів, ідентифікація загроз і вразливостей, формування вимог до системи ІБ, реалізація заходів, вибір засобів і засобів контролю). У контексті ситуаційного підходу ОЗІБ підприємства має базуватися на аналізі ситуації, тобто конкретного складу внутрішніх і зовнішніх факторів, що впливають на організацію в даний момент.

До внутрішніх факторів відносяться наступні фактори: мета і завдання підприємства в області інформаційних систем, структура, використовувані технології і люди (поведінка окремих осіб, членів групи, керівників). Зовнішні фактори можуть змінюватися залежно від випадку, але в основному це такі: фактори прямого впливу (національна політика, регулятивна підтримка, позиції споживачів, партнерів, конкурентів) і непрямі фактори впливу (економічні

умови, наукові розробки) і технологічний прогрес, політичні та міжнародні заходи тощо).

Цікавим є бачення західних вчених, згідно з яким ОЗІБ як складова загальної системи ЗІБ має здійснюватися за схемою «шість «Р»:

- планування (Planning) - діяльність, необхідна для підтримки проектування, створення і реалізації стратегій ІБ;

- політика (Policy) - сукупність організаційних засад, які встановлюють певну поведінку в межах організації;

- програми (Programs) ІБ, які спеціально управляються як окремі об'єкти;

- захист (Protection) - діяльність з управління ризиками, включаючи оцінку і контроль ризиків, механізмів захисту, технологій та інструментів;

- люди (People) - включає в себе забезпечення безпеки персоналу і власне персонал, задіяний у системі ІБ;

- управління проектами (Project Management) - визначення та контроль ресурсів, залучених для реалізації проектів із ЗІБ, вимірювання результатів та корегування заходів.

На думку фахівців, організаційну структуру системи забезпечення ІБ підприємства можна представити у вигляді сукупності таких рівнів:

- рівень 1 - керівництво організації;

- рівень 2 - підрозділ ОІБ;

- рівень 3 - адміністратори штатних і додаткових засобів захисту;

- рівень 4 - відповідальні за ОІБ в підрозділах (на технологічних ділянках);

- рівень 5 - кінцеві користувачі і обслуговуючий персонал.

Крім того, інформаційна безпека організації може бути скомпрометована третіми особами та сторонніми організаціями, зокрема партнерами та тими, хто має на меті втручатися у функціональність системи ІБ або отримати несанкціонований доступ до локальної та віддаленої інформації.

Розглянемо запропоновані в науці методи визначення спрямованості ОЗІБ. Через призму структурно-функціонального підходу виокремлюють наступні напрями діяльності компанії ОЗІБ: формування та практична реалізація комплексної багаторівневої політики ІБ організації та системи внутрішніх вимог, норм і правил; ІБ організації (відділи, служби, відділи), управління інцидентами, аудит стану інформаційних систем в організації. За сферами діяльності, пов'язаними із засобами індивідуального захисту, компанія виділяє наступні напрямки засобів індивідуального захисту: організація режимів і захисту; взаємодія з носіями конфіденційної інформації; робота з персоналом; організація аналітичної роботи та контролю; комплексне інженерне проектування. з ОЗІБ.

Відповідно до іншого підходу діяльність у межах домену ОЗІБ підприємства включає виконання завдань з циклу управління (планування, організація, контроль, регулювання) та завдань у домені ОЗІБ (обмеження та розмежування доступу, сертифікація та авторизація, робота з персонал).

Підсумовуючи різні наукові методи, можна виділити наступні основні принципи ОЗІБ: Адаптивність, що означає пристосовуваність системи ОЗІБ до швидко мінливих умов і загроз навколо підприємства; Ефективність у прийнятті управлінських рішень; Ефективність, що стосується здатності системи ОЗІБ. Оптимальний баланс між продуктивністю та вартістю - економічна доцільність, при якій розмір вартості військової техніки не може перевищувати величину втрат у разі реалізації потенційної загрози.

Крім того, ОЗІБ має бути невід'ємною частиною системи управління організацією, узгодженою з її бізнес-місією та стратегією, централізовано впровадженою за чіткої підтримки та прихильності керівництва організації, гарантуючи повне дотримання керівництвом та працівниками встановлених правил та норм, що регулюють ЗІБ та Облік і моніторинг діяльності в системі ЗІБ із зворотним зв'язком.

ОЗІБ для протидії так званому «людському фактору» негативної діяльності має базуватися на мінімізації індивідуальної відповідальності, розподілі обов'язків і

привілеїв, постійному навчанні та обізнаності персоналу, формуванні організаційної відданості та уникненні дисциплінарних підходів. Важливою умовою успішного проведення ОЗІБ є створення багаторівневої системи захисту, багаторазових засобів захисту та посилення найслабшої ланки.

2.3 Висновки

У даному розділі кваліфікаційної роботи була проведена побудова системи захисту персональних даних для підприємства ТОВ «ПФСОФТ». Для досягнення високого рівня безпеки та захисту ПД були використані апаратне, програмне та організаційне забезпечення.

При обстеженні об'єкту охорони було виявлено низку проблем у реалізації безпеки персональних даних. Серед них:

• відсутність системи обмеження контролю доступу до приміщення, окрім офіс-менеджеру.

• застарілі методи шифрування персональних даних, які зберігаються на сервері – реалізовано за допомогою базового програмного забезпечення.

• зв'язок між співробітниками здійснюється через мережу інтернет в умовах дистанційної роботи, що призводить до підвищеного ризику витоку даних

• антивірусне програмне забезпечення є застарілим.

У рамках даного розділу частини було запропоновано наступні дії:

1. Встановлення системи контролю доступу до приміщення через комбінацію відбитків пальців та розпізнавання обличчя, що дозволить автоматизувати систему доступу до приміщень та нівелювати проблеми використання цих методів контролю доступу окремо одне від одного.

2. Встановлення на ПЕОМ менеджеру з персоналу, директору та офіс-менеджеру систему запуску з захищеного носія, що дозводить обмежити доступ до ПЕОМ цих людей від несанкціонованого доступу.

3. Оновлення антивірусних програм на усіх ПЕОМ корпоративної мережі, що дозволить підвищити рівень захисту даних у корпоративній мережі від шкідливого програмного забезпечення. Наоптимальнішими антивірусними програмами є Norton або mcAfee.

4. Встановлення файрволл-системи (оптимальні варіанти: pfSense або Fortinet FortiGate) для захисту офісної мережі від інтернет-загроз.

5. Використання VPN-сервісу Nord для забезпечення захисту даних, які циркулюють у мережі між працівниками підприємства в умовах дистанційної роботи.

6. Використання системи створення електронного підпису DocuSign Для забезпечення контролю цілісності даних.

7. Проведення щорічних аудитів системи безпеки підприємства на предмет вразливостей.

8. Обов'язкова щоквартальна заміна діючих паролей, яку здійснює системний адміністратор.

3 ЕКОНОМІЧНА ЧАСТИНА

В основі будь-якої діяльності, висвітлення будь-якого питання, або для вирішення будь- якої задачі лежить цільовий підхід. Найбільш повно проявляються переваги цільового підходу при управлінні процесом створення нової техніки, технології, форм і методів створення систем захисту персональних даних на підприємстві. Ефективне виконання поставлених перед працівниками, відповідальними за збереження та нерозголошення персональних даних завдань і об'єктивна оцінка їх діяльності повинні базуватися на чітко сформульованих і чітко визначених системах цілей. Мета - це бажаний результат, обумовлений потребами підприємства, конкретними вимогами замовників до нерозголошення тих чи інших показників тощо. Однією з складових частин цільового підходу є економічний аналіз.

В роботі запропоновано підхід до створення системи захисту персональних даних підприємства ТОВ «ПФСОФТ». Метою даного розділу є обґрунтування економічної доцільності створенної системи захисту персональних даних. Для досягнення цієї мети необхідно визначити:

– величини капітальних витрат на розробку запропонованої системи та експлуатаційних витрат на її реалізацію;

– економічний ефект від впровадження запропонованої системи;

– розрахунок ймовірних збитків.

3.1 Розрахунок капітальних витрат на створення системи захисту персональних даних

Капітальні (фіксовані) витрати – це витрати, підприємства на створення та налаштування системи захисту персональних даних на придбання основних засобів :

- Сервера;
- Комп'ютерна техніка;

- Системи сигналізації та охорони;
- Сейфи;
- Системи обмеження доступу;

Передбачається, що використання цього обладнання (основних засобів) відбуватися протягом терміну їх придатності, а витрачання коштів на них буде проводитися через амортизаційні відрахування. [18]

Капітальні (фіксовані) витрати називаються так, тому, що робляться, як правило, один раз, на початкових етапах створення того чи іншого. В нашому випадку – створення систем захисту персональних даних

До капітальних витрат при створенні систем захисту персональних даних, також слід віднести такі витрати:

- вартість розробки і впровадження ситем захисту;
- залучення, у разі потреби, зовнішніх консультантів.

Витрати на розробку та створення систем захисту, визначаються із трудомісткості в цілому та трудомісткості кожної конкретної операції, з яких складається розробка та впровадження систем захисту.

Трудомісткість розробки системи захисту персональних даних на підприємстві ТОВ «ПФСОФТ» визначається тривалістю кожної робочої операції, до яких можливо віднести наступні:

- тривалість складання завдання для забезпечення захисту персональних даних, які застосовуються на підприємстві, (2 юриста протягом двох робочих днів) $t_{тсз}$=32 години;
- тривалість аналізу можливих загроз для безпеки персональних даних, (менеджер по роботі з персоналом, системний адміністратор, юрист протягом двох робочих днів) $t_{аз}$=48 годин;
- тривалість моделювання систем захисту для електронних баз даних, (спеціаліст з розробки та тестуванню комп'ютерних програм: 5 спеціалістів протягов 3 робочих днів) $t_{мс}$=120 годин;

– тривалість вивчення законодавчих актів, літературних джерел за темою тощо, (юрист, менеджер по роботі з персоналом протягом 1 робочого дня) $t_{вз}$=32 години;

– тривалість оцінки створенної системи захисту персональних даних, (керівник та фінансист – 1 робочий день) $t_{ос}$=16 годин;

– тривалість документального оформлення запропонованої системи захисту (спеціаліст з розробки та тестування 1 робочий день), $t_{до}$=8 годин.

Таким чином, трудомісткість розробки складає:

$$t = t_{тсз} + t_{аз} + t_{мс} + t_{вз} + t_{ос} + t_{до} \quad (3.1)$$

$$t=32+48+120+32+16+8= 256 \text{ годин}$$

Витрати на розробку системи захисту персональних даних на підприємстві ТОВ «ПФСОФТ» ($К_{рсз}$) складаються з витрат на заробітну плату спеціалістів, які беруть участь у процесі створення системи захисту персональних даних $З_{сз}$ і вартості витрат машинного часу, який необхідний для розробки та тестування запропонованої системи $З_{мч}$.

$$К_{рсз} = З_{сзп} + З_{мч} \quad (3.2)$$

$$К_{рсз} = 60276,36 + 1146,88=61423,24 \text{ грн.}$$

$$Зсзп = t\ Зсзп \quad (3.3)$$

$$К_{рсз} = 256 \text{ х } 235,45 = 60276,36 \text{ грн..}$$

де t – загальна тривалість розробки та тестування системи захисту, годин;

Зсзп – средньогодинна заробітна плата спеціалістів, задіяних у створенні системи захисту, визначена у відповідності до Порядку « Обчислення середньої заробітної плати», затвердженого Постановою Кабінету Міністрів України від 8 лютого 1995 р. N 100 [17] і складає 235,45 грн. (414400,00 : 10:176 =235,45 грн).

Фонд заробітної плати на підприємстві на місяць становить 414400,00 грн., середньоспискова чисельність штатних працівників 10 одиниць, фонд робочого часу за місяць – 176 годин.

Вартість машинного часу для розробки системи захисту на ПК визначається за формулою:

$$З_{мч} = t \times С_{мч} \quad (3.5)$$

$$З_{мч} = 256 \times 4,48 = 1146,88 \text{ грн.}$$

де t – трудомісткість створення системи захисту на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначена згідно з середнім значенням споживаної потужності ПК та вартості електричної енергії . В нашому випадку $С_{мч}$ становить 4,48 грн./год.

Капітальні витрати на налагодження системи захисту персональних даних, визначені за формулою:

$$КВ = К_{зпз} + К_{пз} + К_{аз} + К_{навч} \quad (3.6)$$

де $К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового ПЗ, грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу.

Всі дані мають відображення в регістрах бухгалтерського обліку, які в подальшому мають відображення в «Звіті про фінансові результати малого підприємства» і складають 4300,00 [16]

Таким чином, капітальні (фіксовані) витрати на розробку системи захисту персональних даних становлять:

$$К = К_{рсз} + КВ \quad (3.7)$$

$$К = 61423,24 + 4300,00 = 65723,24 \text{ грн.}$$

де $К_{рсз}$ – вартість розробки систем захисту персональних даних, 61423,24 грн;

КВ - Капітальні витрати на налагодження системи захисту персональних даних

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи захисту персональних даних складають:

$$С = С_в + С_к + С_{ак} \quad (3.8)$$

де $С_в$ - вартість відновлення й модернізації системи ($С_в = 0$), вона функціонує на підприємстві. Відновлення та модернізація на даний момент часу не потрібна;

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_з + С_{єсв} + С_{ел} + С_{тос} \quad (3.9)$$

Річний фонд заробітної плати персоналу, що обслуговує систему захисту персональних даних ($С_з$), складає:

$$С_з = З_{осн} х 12 \quad (3.10)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу. Основна заробітна плата одного спеціаліста задіяного в обслуговуванні системи захисту персональних даних на місяць складає 31080 грн. Виконання роботи щодо обслуговування системи захисту персональних даних на підприємстві потребує 15% робочого часу

Отже,

$$С_з = (31080{,}00 \text{ х } 0{,}15) \times 12 = 55944{,}00 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників податків з 01.01.2021 р. складає 22%.

$$С_{єсв} = 55944{,}00 \times 22\% = 12307{,}68 \text{ грн.}$$

Вартість електроенергії, що споживається ПК та іншими системами керування доступом до баз даних ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \times F_р \times Ц_е \quad (3.11)$$

де Р – встановлена потужність систем захисту баз даних (ПК, сервера, системи охорони та керування доступом), (Р=2,5 кВт);

$F_р$ – річний фонд робочого часу системи захисту 8760 годин (365 днів х24 год.);

$Ц_е$ – тариф на електроенергію, 1,40 грн. (1,68 грн./кВт за годину період з 7 -00 по 23-00 та тариф 0,84 з 23-00 до 7-00).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 2,5 \text{ х } 8760 \times 1,40 = 30660,00 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи захисту персональних даних визначаються у відсотках від вартості капітальних витрат – 3%

$$С_{тос} = 65723,24 \times 3\% = 1971,70 \text{ грн.}$$

Витрати на керування системою інформаційної безпеки складають:

$$С_к = 55944,00 + 12307,68 + 30660,00 + 1971,70 = 100883,38 \text{ грн.}$$

Таким чином, сума поточних витрат обслуговування та експлуатації систем захисту персональних даних по ТОВ «ПФСОФТ» складає:

$$С = С_в + С_к + С_{ак} \qquad (3.12)$$

$$С = 0 + 100883,38 + 0 = 100883,38 \text{ грн.}$$

3.3 Оцінка можливого збитку від витоку персональних даних

Для розрахунку вартості збитку від втрати конфіденційності персональних даних необхідно мати наступні умовні величини:

$t_п$ – час простою, внаслідок втрати інформації про персональні дані - 2 години (час потрібний для відновлення);

$t_{ви}$ – час повторного введення загубленої інформації- 3 години;

$t_в$ – час для відновлення роботи системи після завантаження даних - 1 година;

$З_п$ – заробітна плата персоналу, задіяного в системі захисту 31080,00 грн./міс.;

$Ч_о$ – чисельність персоналу (менеджер по роботі з персоналом, спеціаліст з розробки та тестуванню комп'ютерних програм), 2 особи;

I – число атакованих сегментів баз даних (паперові носії, електронні носії)- 2;

N – середнє число атак на рік, 36.

Збитки від втрати конфіденційності даних становять:

$$U = П_п + П_в \quad (3.13)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого баз даних, грн;

$П_в$ – вартість відновлення баз даних (введення втраченої інформації, перезапуск систем безпеки та ін.), грн;

Втрати від зниження продуктивності праці – це оплата простою працівників:

$$П_п = \frac{З_п}{F} \times t_п \quad (3.14)$$

$$П_п = \frac{31080{,}00 \times 2}{176} \times 2 = 706{,}36 \text{ грн.}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення роботи системи захисту:

$$П_в = П_{ви} + П_{пв} \quad (3.15)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення роботи бази даних, грн;

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників, які задіяні у відновлення та повторному введені інформації в бази даних Зп, з урахуванням необхідного для цього часу $t_{ви}$.

Отже:

$$П_п = \frac{З_п}{F} \times t_{ви} \quad (3.16)$$

$$П_п = \frac{31080,00 \times 2}{176} \times 3 = 1059,54 \text{ грн.}$$

Витрати на відновлення роботи бази даних та системи її захисту $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати персоналу :

$$П_п = \frac{З_п}{F} \times t_в \quad (3.17)$$

$$П_п = \frac{31080,00 \times 2}{176} \times 1 = 353,18 \text{ грн.}$$

Тоді витрати на відновлення роботи системи захисту та баз даних складуть:

$$П_в = 1059,54+353,18 = 1412,72 \text{ грн.}$$

$$U = 706,36+1412,72= 2119,08 \text{ грн.}$$

Виходячи з наданих вихідних даних та проведених розрахунків вартість збитків від витоку персональних даних на підприємстві ТОВ «ПФСОФТ» складає:

$$В= 2 \times 36 \times 2119,08= 152573,76 \text{ грн.}$$

3.4 Загальний ефект від впровадження системи захисту персональних даних

Загальний ефект від впровадження системи захисту персональних даних з урахуванням ризиків витоку інформації:

$$E = B \cdot R - C \quad (3.18)$$

де B – загальний збиток від атаки у витоку інформації, грн.;

R – вірогідність успішної реалізації загрози витоку даних 80%;

C – сума щорічних поточних витрат наобслуговування та експлуатації систем захисту персональних даних по ТОВ «ПФСОФТ» складає:

Загальний ефект від застосування системи захисту персональних даних ризиків та витрат складає:

$$E = 152573,76 \text{ x } 0,8 - 100883,38 = 21175,63 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності системи захисту персональних даних

«Сукупна вартість володіння або вартість життєвого циклу (англ. total cost of ownership, TCO) — загальна величина цільових витрат (прямих та непрямих), які вимушений нести власник з моменту вступу в право власності на певний продукт чи систему до моменту виходу з права власності та виконання власником зобов'язань, пов'язаних з володінням, у повному обсязі».

За методикою сукупної вартості володіння (ТСО) можна визначити показники економічної ефективності системи інформаційної безпеки персональних даних, а саме:

коефіцієнт повернення інвестицій (ROSI);

термін окупності капітальних інвестицій (T_o).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи захисту персональних даних:

$$ROSI = \frac{E}{K} \tag{3.19}$$

де E – загальний ефект від впровадження ситеми захисту персональних даних грн.;

К – капітальні інвестиції , грн.

Коефіцієнт повернення інвестицій ROSI на прикладі підприємства підприємстві складає:

$$ROSI = \frac{21175,63}{65723,24} = 0,32, \text{ частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > \frac{(Nдеп - Nінф)}{100} \tag{3.20}$$

де $N_{деп}$ – річна депозитна ставка, 4,75% за 2022 рік;

$N_{інф}$ – річний рівень інфляції, 26,6% за 2022 рік [17]

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,32 > (4,75 – 26,6)/100 = 0,32 > - 0,22.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи захисту персональних даних:

$$T_o = \frac{K}{E} \quad (3.21)$$

Тобто загальний ефект від впровадження системи захисту персональних даних береться у спввідношенні до капітальних інвестицй. (ціле до частки):

$$T_o = \frac{1}{0,32} = 3,13$$

Термін окупності капітальних інвестицій складає на підприємстві 3,13 років.

3.6 Висновки

Із всього вищевикладеного, можна зробити висновок, розробка системи захисту персональних даних на підприємстві ТОВ «ПФСОФТ» є економічно доцільною, про що свідчать, зокрема : коефіцієнт повернення інвестицій ROSI складає 0,32 грн.. (тобто на 1 гривню капітальних витрат припадає 0,32 грн. економічного ефекту). При цьому загальний економічний ефект від застосування системи захисту персональних даних ризиків та витрат складає 21175,63 грн.

Термін окупності при цьому складатиме 3,13 років. А капітальні інвестиції визначено обсягом 65723,24 грн

ВИСНОВКИ

У роботі було розглянуто ключові питання, пов'язані з ризиками для безпеки персональних даних. Аналізуються потенційні загрози, такі як шкідливе програмне забезпечення, хакерські атаки, витоки інформації та недбалість персоналу, що можуть призвести до порушення безпеки даних. Також було розглянуто основні юридичні моменти супроводу безпеки персональних даних та наведено список основнх документів, які регулюють положення щодо безпеки персональних даних на території України та країн ЄС,

У дослідженні також проаналізовані та запропоновані методи та основні напрями захисту персональних даних. Розглядаються технологічні засоби, які можуть бути використані для захисту, зокрема шифрування даних, використання мережевих брандмауерів та антивірусного програмного забезпечення, а також системи контролю доступу. Окрім технологічних аспектів, вивчаються організаційні заходи, включаючи політики безпеки, навчання персоналу та встановлення процедур контролю, що сприяють підвищенню рівня захисту персональних даних.

Результат зроблених у цій роботі обчислень у економічному розділі можуть чітко показати, що запропоновані методи захисту персональних даних на підприємстві є економічно ефективними.

ПЕРЕЛІК ПОСИЛАНЬ

1. ЗАКОН УКРАЇНИ “Про захист персональних даних”. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

2. ЗАКОН УКРАЇНИ “Про захист інформації в інформаційно-комунікаційних системах”. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

3. Конституція України. [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/constitution

4. ЄВРОПЕЙСЬКА КОНВЕНЦІЯ З ПРАВ ЛЮДИНИ. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_004#Text

5. ЗАКОН УКРАЇНИ “Про інформацію”. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

6. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/994_326#Text

7. Кодекс законів про працю України. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/322-08#Text

8. Муха А. В науковий керівник: Павлюх М. В. ЗАГРОЗИ ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ / Серія «Міжнародні відносини». Випуск 5 / УДК: 316.472.4:342.7:001.103-027.552:004.451.5

9. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни і визначення. - К.: Держстандарт України, 1998. 8. Закон України «Про державну таємницю». – К.: Відомості Верховної Ради України, 1994. - N 16. - Ст. 93.

10. ЄВРОПЕЙСЬКА КОНВЕНЦІЯ З ПРАВ ЛЮДИНИ. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/995_004#Text

11. РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з

опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

12. Кібербезпека: як подбати про захист персональних даних компанії від атак? [Електронний ресурс]. – Режим доступу: https://mklegalservice.com/tpost/egijjim6h1-kberbezpeka-yak-podbati-pro-zahist-perso

13. Antivirus maker Avast shuts down data collection firm after controversy. [Електронний ресурс]. – Режим доступу: https://www.cnet.com/news/privacy/antivirus-company-avast-closes-analytics-company-over-data-privacy-scandal/

14. Open Crypto Audit Project TrueCrypt Cryptographic Review [Електронний ресурс]. – Режим доступу: https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf

15. ДСТУ 3396.1-96. [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf

16. Додаток 1 до Положення (стандарту) бухгалтерського обліку 25 «Фінансовий звіт суб'єкта малого підприємництва» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0161-00#Text

17. Постанова від 8 лютого Про затвердження Порядку обчислення середньої заробітної плати. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/100-95-%D0%BF#Text

18. Про затвердження Національного положення (стандарту) бухгалтерського обліку 25 "Спрощена фінансова звітність". [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0161-00#Text

19. Інфляція в Україні у 2022 році склала 26,6% – Держстат. [Електронний ресурс]. – Режим доступу: https://www.epravda.com.ua/rus/news/2023/01/10/695830/#:~:text

20. Філоненко, С. Ф. Система попередження витоку персональніх даних мережевими каналами [Текст] / С. Ф. Філоненко, І. М. Мужик, Т. В. Німченко //81Ukrainian Scientific Jornal of Information Security. – 2014. – Vol. 20, № 3. – P.279–285.

21. 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. – №3–4. – С. 199–203.

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

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	37	
6	А4	Спеціальна частина	39	
7	А4	Економічний розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
13	А4	Додаток Д	1	

ДОДАТОК Б. Наказ «Про запровадження дистанційної роботи»

ТОВАРИСТВО З ОБМЕЖЕННОЮ ВІДПОВІДАЛЬНІСТЮ «_ПФСОФТ_»

НАКАЗ № __1_____

м. Дніпро 24.02. 2022 р.

Про запровадження дистанційної роботи

У зв'язку з військовою агресією Російської Федерації проти України та запровадженням воєнного стану згідно з Указом Президента України «Про введення воєнного стану в Україні» від 24.02.2022 р. № 64/022 та керуючись ст. 60-2 «Дистанційна робота» Кодексу законів про працю України

НАКАЗУЮ:

1. Запровадити дистанційну роботу для працівників підприємства (згідно з Додатком до цього наказу) з 24.02.2022 р. до закінчення воєнного стану строком на 30 (тридцять) діб до 25.03.2022 р. включно.

2. Контроль за виконанням цього наказу залишаю за собою.

Директор _____

ДОДАТОК В. Перелік документів на оптичному носії

1 Презентація Жевтіло.ppt

2 Диплом Жевтіло.doc

ДОДАТОК Г. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («_____»).

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Д. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-19-2 Жевтіло Ю.Ю.

на тему: «Побудова моделі захисту персональних даних на підприємстві ТОВ «ПФСОФТ»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 106 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на побудову моделі ефективного захисту персональних даних на прикладі підприємства.

При виконанні роботи автор продемонстрував відмінний рівень теоретичних знань і практичних навичок. На основі аналізу правового супровіду захисту персональних даних та можливих загроз щодо безпеки персональних даних в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було побудовано систему захисту персональних даних для підприємства ТОВ «ПФСОФТ». Для досягнення високого рівня безпеки та захисту ПД було використане апаратне, програмне та організаційне забезпечення.

Практична цінність роботи полягає у тому, що запропоновані рішення можуть бути використані для організації захисту персональних даних на інших підприємствах.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Жевтіло Ю.Ю. заслуговує на оцінку «_____» та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доцент **О.В. Герасіна**