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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Шушпанової Анастасії Русланівни*

академічної групи *125м-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Особливості впровадження вимог загального регламенту захисту даних (GDPR) в разі використання хмарних технологій*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Шушпанова А.Р.* **академічної групи** *125-м-17-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Особливості впровадження вимог загального регламенту захисту даних (GDPR) в разі використання хмарних технологій*

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.2018 № 2025-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *Захист персональних даних*

Предмет досліджень *Особливості впровадження вимог загального регламенту захисту даних (GDPR) в хмарних технологіях обробки інформації*

Мета *Зменшення вірогідності витоку персональних даних шляхом впровадження вимог загального регламенту захисту даних*

Вихідні дані для проведення роботи *Вітчизняна та міжнародна правова база у сфері інформаційної та кібербезпеки, наукові публікації вітчизняних та іноземних авторів, статистичні дані , результати науково-дослідницької та переддипломної практик*

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна *полягає у визначенні загальних складових рекомендацій щодо впровадження загального регламенту захисту даних*

Практична цінність *полягає у розробці рекомендації щодо впровадження загального регламенту захисту даних для власників інформації*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати роботи мають відповідати вимогам чинного законодавства України та мають підвищити рівень обізнаності користувачів у питанні захисту персональних даних

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Огляд джерел за темою та напрям досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-24.11.18
Виконання економічного розділу	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *від реалізації результатів роботи очікується позитивним завдяки зниженню можливих збитків через порушення вимог загального регламенту захисту даних завдяки створенню та впровадженню рекомендацій для власників інформації щодо впровадження регламенту, що запропоновані у дипломній роботі*

Соціальний ефект *дипломної роботи полягає у підвищенні обізнаності керівництва та працівників підприємства у питаннях чинного законодавства у сфері захисту персональних даних та ефективності забезпечення безпеки інформації*

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення пояснювальної записки:

ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення»;

Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / О.Ю. Гусєв, О.В. Герасіна, О.М. Алексєєв, О.В. Кручінін – Дніпро:НГУ, 2018. – 52с;

Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: І.В. Шереметьєва, Д.П. Пілова, Н.М.

Романюк. – Дніпро: Національний технічний університет "Дніпровська політехніка",2017. – 17 с.

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 60 с., 5 рис., 1 табл., 4 додатки, 37 джерел.

Об’єкт дослідження: захист персональних даних.

Предмет дослідження: особливості впровадження вимог загального регламенту захисту даних (GDPR) в хмарних технологіях обробки інформації.

Мета дипломної роботи: зменшення вірогідності витоку персональних даних шляхом впровадження вимог загального регламенту даних.

У першому розділі проведено дослідження принципів хмарного обчислення даних та виділено три основні моделі обслуговування. Був проведений аналіз поточної ситуації в Україні в галузі безпеки персональних даних. Проаналізовано сценарії кіберзлочинів за останній період.

Розглянуто нормативно-правову базу у сфері захисту інформації. Виділені основні закони, нормативні документи та державні стандарти, що стосуються розробки політики безпеки інформації на підприємстві.

У другому розділі було визначено основні етапи впровадження вимог загального регламенту захисту даних на прикладі однієї з трьох основних моделей обчислення хмарних технологій — SaaS. Визначено особливості цього методу.

Було розглянуто три способи збереження даних з різними видами шифрування. Відповідно до них було проведено аналіз інформаційних ризиків та визначено оптимальній спосіб збереження даних. Розроблено рекомендації щодо впровадження загального регламенту захисту даних, дотримуючись попередніх досліджень.

В економічній частині проведений розрахунок капітальних та експлуатаційних витрат на розробку і впровадження рекомендації по застосуванню GDPR.

Новизна очікуваних результатів полягає у визначенні загальних складових рекомендацій щодо впровадження загального регламенту захисту даних.

ІНФОРМАЦІЙНА БЕЗПЕКА, ПЕРСОНАЛЬНІ ДАНІ, ВИТІК ПЕРСОНАЛЬНИХ ДАНИХ, ХМАРНІ ТЕХНОЛОГІЇ, GDPR, РЕКОМЕНДАЦІЇ ДЛЯ ВЛАСНИКІВІНФОРМАЦІЇ

РЕФЕРАТ

Пояснительная записка: 50 с., 4 рис., 2 табл., 4 приложения, 36 источников.

Объект исследования: защита персональных данных.

Предмет исследования: особенности внедрения требований общего регламента защиты данных (GDPR) в облачных технологиях обработки информации.

Цель дипломной работы: уменьшение вероятности утечки персональных данных путем внедрения требований общего регламента данных.

В первой главе проведено исследование принципов облачного вычисления данных и выделено три основных модели обслуживания. Был проведен анализ текущей ситуации в Украине в области безопасности персональных. Приведенные примеры крупнейших случаев киберпреступлений за последний период.

Рассмотрены нормативно-правовую базу в сфере защиты информации. Выделены основные законы, нормативные документы и государственные стандарты, касающиеся разработки политики безопасности информации на предприятии.

Во втором разделе были определены основные этапы внедрения требований общего регламента защиты данных на примере одной из трех основных моделей вычисления облачных технологий - SaaS. Определены особенности этого метода.

Были рассмотрены три способа хранения данных с различными видами шифрования. Согласно им был проведен анализ информационных рисков и определены оптимальной способ хранения данных.

Разработаны рекомендации по внедрению общего регламента защиты данных, соблюдая предыдущих исследований.

В экономической части произведен расчет капитальных и эксплуатационных затрат на разработку и внедрение рекомендации по применению GDPR.

Новизна ожидаемых результатов заключается в определении общих составляющих рекомендаций по внедрению общего регламента защиты данных.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ, УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБЛАЧНЫЕ ТЕХНОЛОГИИ, GDPR, РЕКОМЕНДАЦИИ ДЛЯ ВЛАДЕЛЬЦЕВ ИНФОРМАЦИИ

ABSTRACT

Explanatory note: 59 p., 5 fig., 2 tab., 4 appendices, 32 sources.

Object of study: protection of personal data.

Subject of research: features of the implementation of the requirements of the General Data Protection Regulations (GDPR) in cloud information processing technologies.

The purpose of the thesis: reducing the likelihood of leakage of personal data by implementing the requirements of the general data regulations.

The first chapter examines the principles of cloud computing and highlights three main service models. An analysis was made of the current situation in Ukraine in the field of personal security. Examples of the largest cases of cybercrime in the last period.

Considered the regulatory framework in the field of information security. Highlighted the main laws, regulations and state standards relating to the development of information security policy in the enterprise.

In the second section, we identified the main stages of implementing the requirements of the general data protection regulations using the example of one of the three main cloud computing models - SaaS. The features of this method are determined.

Three ways of storing data with different types of encryption were considered. According to them, information risk analysis was carried out and the optimal data storage method was determined.

Developed recommendations for the implementation of general data protection regulations, following previous studies.

In the economic part, the calculation of capital and operating costs for the development and implementation of recommendations for the application of GDPR.

The novelty of the expected results consists in determining the general components of the recommendations for the implementation of the general data protection policy.

INFORMATION SECURITY, PERSONAL DATA, PERSONAL DATA BREACH, CLOUD TECHNOLOGIES, GDPR, RECOMMENDATIONS FOR OWNERS OF INFORMATION

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ЄС	–	Європейський Союз
ІТ	–	інформаційні технології
ІБ	–	інформаційна безпека
ПД	–	персональні дані
ПЗ	–	програмне забезпечення
ОС	–	операційна система
GDPR	–	General Data Protection Regulation
DPA	–	Data Processing Agreement
DPO	–	Data Protection Officer
DPIA	–	Data Protection Impact Agreement
NIS	–	Network and Information Security
ISO	–	International Organization for Standartization
IaaS	–	infrastructure as a service
PaaS	–	platform as as service
SaaS	–	software as a service

ЗМІСТ

ВСТУП

В умовах сучасного розвитку інформаційних технологій та середовища, нагальним питанням постає безпека інформаційних ресурсів. Те, що з одного боку спрощує та підвищує ефективність введення бізнесу, з іншого потребує сталих та регламентованих правил поводження з інформацією аби запобігти матеріальним збиткам. Слід зауважити, що в рамках нестабільної економічної ситуації в країні керівництво організацій нерідко зневажає потребу у створенні та підтримці системи захисту інформації.

Однією із найважливіших вимог забезпечення сталого функціонування будь-якого підприємства є надійність роботи інформаційної системи та зовнішніх інформаційних ресурсів в мережі Internet.

Особливої уваги слід приділити даним, що стосуються напряму користувачів системи або ресурсу. Іншим словом — будь-якої інформації, що може ідентифікувати людину — персональним даним (ПД).

З обробкою персональних даних сьогодні ми стикаємося повсюди: соціальні мережі, онлайн-банкінг та ін. Інтернет-ресурси. Безпека та надійність мають стати ключовими факторами як для володільців ресурсу так і для користувачів.

Відповідний заданим вимогам рівень інформаційної безпеки (ІБ) може бути досягнутий виключно за умови комплексного підходу, що містить у собі програмні, апаратні та організаційні міри захисту. Доволі часто останніми нехтують, хоча вони є найбільш вагомими та в середньому повинні складати більше 50% від усіх заходів у цьому напрямку.

Першим, на що слід звертати увагу в цьому питанні це нормативно-правова база. Важливими є не тільки національні постанови, а й міжнародні (європейські). Особливо, якщо ресурсом користуються або можуть користуватися громадяни країн членів ЄС. Відповідність всім чинним нормам законодавства підвищує рівень довіри та лояльності до ресурсу. Зазвичай, мотивами для створення політики безпеки персональних даних є: додержання вимог чинного законодавства, виконання вимог керівництва організації, клієнтів або їх партнерів, підвищення конкурентоспроможності на ринку, підготовка до міжнародних сертифікацій, позбавлення зауважень аудиторів, економічна доцільність тощо.

Стає очевидним, що приділення уваги до безпеки персональних даних являється фундаментальною частиною побудови режиму інформаційної безпеки для організації ефективної роботи структури будь-якого типу та масштабів. Це зводить до мінімуму наслідки не коректних або випадкових дій людини у системі, сприяє створенню культури інформаційної безпеки та дисциплінує співробітників компанії.

РОЗДІЛ 1.
СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз особливостей застосування хмарних технологій

Сьогодні майже неможливо зустріти людину, яка би не користувалася хмарними технологіями у повсякденному житті. Починаючи з ранкової пошти, що є додатком у вашому смартфоні та закінчуючи особливим програмним забезпеченням на роботі, цей принцип обчислення оточує нас скрізь. Майже неможливим стає переоцінити його значущість, а разом з тим зростає потреба розібратися в усіх перевагах, недоліках та особливостях безпеки інформації у віддаленому середовищі.

Хмарні технології (обчислення) — це надання обчислювальних послуг за вимогою — від додатку до сховищ та обчислювальних потужностей. Зазвичай це здійснюється за допомогою Інтернету та на платній основі.

Замість того, аби мати власну обчислювальну інфраструктуру або центри обробки даних, компанії можуть орендувати доступ до будь-чого у постачальника хмарних послуг.

Однією з переваг використання послуг хмарних технологій є те, що компанії можуть уникнути початкових витрат та складностей, пов'язаних із володінням та обслуговуванням власної IT-інфраструктури та замість цього платити лише за те, що вони використовують в конкретний період.

У свою чергу, постачальники таких послуг отримують вигоду за рахунок значної економії через масштаби, надаючи однакові послуги широкому колу клієнтів.

Хмарні обчислення є основою величезної кількості послуг. Вони включають в себе як повсякденні сервіси (Gmail, або резервне копіювання фото у хмарному сховищі) так і сервіси, що дозволяють великим компаніям розміщувати всі свої дані та запускати всі свої додатки в хмарі.

Хмарні технології стають опцією за змовчуванням для багатьох додатків: постачальники програмного забезпечення все частіше пропонують свої додатки у виді послуг через Інтернет, а не у вигляді автономних продуктів. Перш за все через бажання перейти на модель абонентської підписки. Проте, завжди існує потенційний

недолік хмарних обчислень в тому, що вони також можуть призвести до нових затрат та до нових ризиків для компаній, що їх використовують.

Хмарні обчислення можна розділити на три основні моделі обслуговування. IaaS – “інфраструктура як послуга” відноситься до фундаментальних блоків обчислювальної техніки, що можна орендувати: фізичним чи віртуальним серверам, сховищам та мережам. Це є привабливим для компаній, які бажають створювати додатки з самого початку та хочуть самостійно контролювати практично всі елементи створення ПЗ. Дослідження Oracle [5] з'ясували, що дві треті користувачів IaaS заявили, що використання онлайн-інфраструктури полегшує інновації, скорочує час на впровадження нових додатків та послуг та значно скорочує затрати на їх обслуговування. Проте, половина вважає IaaS недостатньо безпечною для більшості важливих даних.

Інша модель називається PaaS – “платформа як послуга”. Це є наступним рівнем, що включає в себе не тільки сховища та віртуальні сервери, а й додаткові інструменти та програмне забезпечення, що необхідні розробникам для створення додатків “зверху”. Наприклад, сюди можуть входити управління базами даних, операційні системи і засоби розробки.

Третя модель обслуговування SaaS – “програмне забезпечення як послуга”. Напевно, це найпоширеніша модель до якої звикла більшість людей у повсякденному житті. Базове обладнання та ОС не мають відношення до кінцевого користувача, що буде звертатися до сервісу за допомогою веб-браузеру чи додатку.

Звісно, багато компанії досі занепокоєні безпекою хмарних сервісів, хоча порушення безпеки в цій сфері зустрічаються доволі рідко. Наскільки безпечним ви вважаєте хмарні обчислювання буде багато в чому залежати від того, наскільки безпечні ваші існуючі системи. Внутрішні системи, котрі управляються командою, якій доводиться піклуватися про багато інших речей, ймовірно будуть мати більше витоку аніж системи, контрольовані інженерами хмарного провайдеру, що займається захистом цієї інфраструктури.

Проте, проблеми з безпекою залишаються, особливо для компаній, що працюють з багатьма хмарними сервісами одночасно. Це призводить до зростання кількості інструментів хмарної безпеки, котрі відстежують переміщення даних “з хмари на хмару”, а також між хмарними платформами. Ці інструменти можуть

ідентифікувати зловмисне використання даних у хмарному сховищі, несанкціоновані завантаження та шкідливі програми.

Очевидно, що питанню захисту інформації при хмарному обчисленні слід приділяти значну увагу, особливо якщо серед цієї інформації є чутливі дані (персональні). Витік такої інформації несе за собою не тільки шкоду репутації компанії, а й чималі наслідки через порушення чинного законодавства у сфері захисту персональних даних.

1.2 Аналіз нормативно-правової бази у сфері захисту персональних даних

З процесом глобалізації та розвитку технологій, бізнесу та промисловості все більшої потреби в собі зазнають інформаційні технології (ІТ) та все що з ними пов’язано. За останні роки світ перейшов на збереження та обмін інформацією через комп’ютерні системи, мережу Інтернет, фізичні носії інформації та інше. Будь-яка сфера діяльності тепер насамперед спирається на використання ІТ, адже вони стали невід’ємною складовою життєдіяльності суспільства.

У сучасному світі інформацію слід ставити на один рівень із матеріальними та енергетичними ресурсами, оскільки вона є важливим показником якісних змін у житті суспільства. Постає питання безпеки інформації та її підтримки і забезпечення за допомогою сучасних методів. Дуже часто інформаційній безпеці приділяється недостатньо уваги, що потім несе за собою важкі наслідки. Економічні збитки, погіршення ділових відносин, погана репутація та недовіра працівників – усе це може відбутися з підприємством, що допустило витік інформації, яка потребувала захисту.

Лише за останній рік в Україні було зафіксовано декілька гучних справ з приводу витоку персональних даних. Деякі з них були спростовані, як витік бази даних користувачів “Нової Пошти” [6], а на деякі було подано колективні позови та проведено слідчі експерименти (несанкціонована передача персональних даних Приватбанку третім особам) [7].

Спираючись на дані дослідження ресурсу Computer Business Review [], протягом першої половини 2018 року кожної секунди було викрадено або спотворено 291 документ.

Нижче наведена діаграма кількості інцидентів за галузями. Ця статистика стосується кількості порушень, а не їх розголосу.

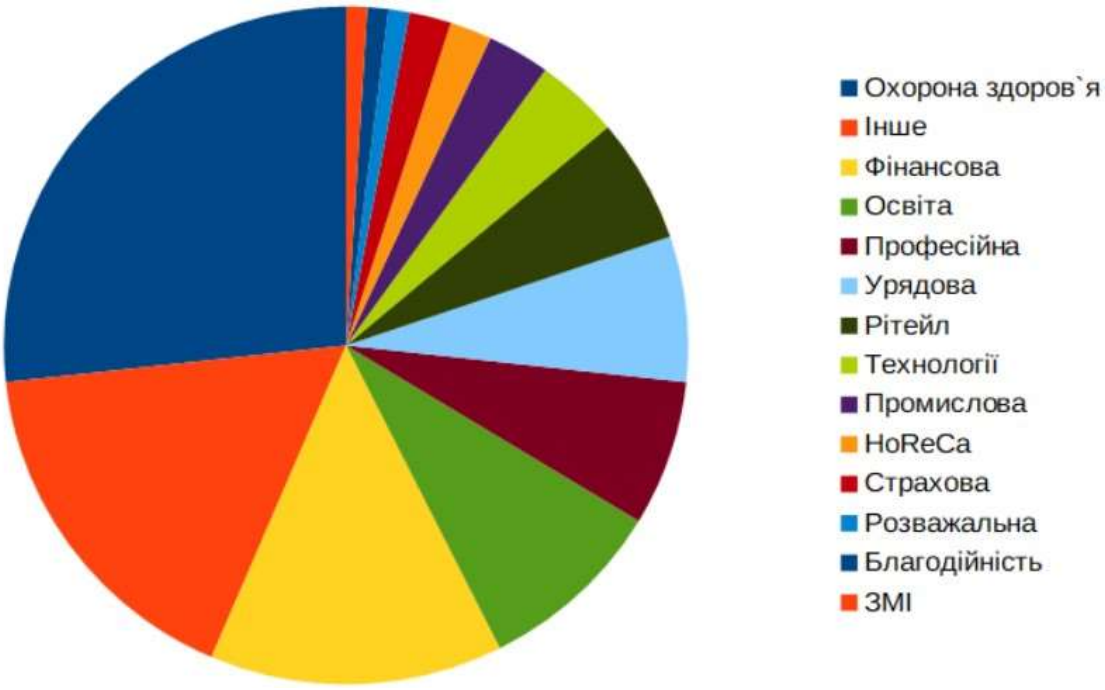

Рисунок 1.1 – Кількість інцидентів витоку інформації за галузями, 2018 рік

На початку другої половини XX сторіччя з розвитком інформаційних технологій значно збільшилась можливість швидше оброблювати інформацію та в набагато більшому обсязі. З 60-х років ця можливість поширюється серед більшого кола людей. Це стало викликати занепокоєність з боку Ради Європи.

Так, у 1968 році Парламентська асамблея видає “Рекомендацію №509” . У ній йдеться про занепокоєння з приводу можливих загроз праву на приватне життя в результаті використання нових технологій обробки даних.

Як наслідок, асамблея вповноважила комітет з прав людини вивчити це питання. Багато людей вважає цей момент як точку відліку для захисту інформації.

Перша відповідь лунає з ФРН, де на землі Гессен через два роки приймають перший в історії закон про персональні дані. Важливим є те, що цей закон був локальним і не діяв на федеральному рівні.

Слідом реагують Сполучені Штати Америки. У 1974 році приймають “Privacy Act” [8], у якому американський конгрес вперше пов'язує право на приватне життя з персональними даними. Цей закон стверджує, що особисте життя може бути напряму порушено в результаті збору, використання та розповсюдження персональної інформації державними органами влади.

Обидва акти не можна назвати повноцінним законом, що регулює обробку персональних даних. Але завдяки їм право на захист персональних даних потроху почало виходити з тіні права на приватне життя.

Піонером у сфері захисту персональної інформації стає саме Німеччина: у 1977 році в ФРН з'являється перший національний закон про захист персональних даних. Особливе відношення німецької громадськості до цього пов'язано в першу чергу з локальними історичними подіями.

Справа в тому, що з 50-х років XX сторіччя на долю німців випало два абсолютно протилежних політичних режими: з одної сторони Третій Рейх, а з іншої ФРН та НДР. Основною засадою цих режимів було масове стеження за населенням.

Такі події призвели до того, що згодом конфіденційність в цій країні вийшла чи не на перший рівень. Саме тому Німеччина досі вважається одним із світових лідерів із захисту приватного життя та персональних даних.

Іншою важливою країною в цій сфері стала Франція, котра відстала від Німеччини лише на один рік. Прийняття в 1978 році закону про інформатику та громадянські свободи [9] також було пов'язано з локальними подіями.

На початку 70-х років французький уряд розробив та запровадив проект SAFARI, сенс якого полягав у створенні єдиного реєстру даних за допомогою використання номеру соціального страхування, що дозволяло ідентифікувати будь-якого громадянина. Обробку всієї цієї інформації планувалося здійснювати шляхом використання найкращих на той момент обчислювальних технологій.

У 1974 році французьке видання Le Monde публікує про це статтю під назвою «SAFARI ou la chasse aux Français» (САФАРІ або полювання на французів), чим провокує гучний скандал на тему масового стеження.

Під дією громадськості уряд був вимушений відступити. Це й призвело до прийняття вищезгаданого закону та створенню комісії з інформатики та громадянських свобод. Тим не менш, запобігти реалізації проекту не вдалося, але комісія змогла встановити певні обмеження на обробку персональних даних.

Французький та німецький закони стають наріжним каменем в області захисту персональних даних та надають значний поштовх для її розвитку. На цю проблему починають звертати увагу все більше країн та міжнародних організацій.

У 1980 році Організація економічного співробітництва та розвитку публікує керівництва [10] з захисту персональних даних з урахування триваючого розвитку комп'ютерних технологій та їх використання у комерційних транзакціях.

Через рік приймають перший міжнародний договір у сфері захисту інформації, їм стає Конвенція про захист фізичних осіб при автоматизованій обробці персональних даних [11]. Конвенція стала великим досягненням в цій сфері. Наразі до неї приєдналася 51 країна.

При цьому, постійно прискорюваний розвиток інформаційних технологій створює нові проблеми у сфері захисту даних та приватності життя. Головною причиною появлення таких проблем стає поява глобальної мережі Інтернет та її швидкого розвитку. Першим потенційну загрозу помічаю Євросоюз, котрий у 1995 році приймає Директиву «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [12].

Основною метою цього закону є адаптація до нових загроз та уніфікування законодавства про захист персональних даних для країн-членів ЄС. Для цього було покращено механізми передбачені міжнародною конвенцією від 1981 р., а також запроваджені нові обов'язки для операторів персональних даних та нові права для громадян ЄС.

Із завершенням 90-х років починають формуватися гіганти-монополісти Інтернету. Їх називають великою п'ятіркою або GAFAM (Google, Amazon, Facebook, Apple, Microsoft). При безпосередній участі згаданих американських корпорацій з'являються нові методи монетизації комерційної діяльності в мережі Інтернет. Пошуковик Google та соціальна мережа Цукерберга не мають прямих джерел капіталізації (на відміну від Amazon чи Microsoft) розпочинають показувати рекламу, що заснована на аналізі поведінки своїх користувачів (таргетинг). Контекстна реклама починає користуватися напрочуд великим попитом і к цій системі згодом приєднуються Amazon, Microsoft та Apple.

Аби реклама якомога довше залишалася релевантною, п'ять вищезгаданих компаній на чолі з Google та Facebook починають збирати величезні масиви даних з користувачів з усього світу. При цьому розвиваються технології, що дозволяють швидко обробляти та аналізувати цю інформацію та знаходити особливості поведінки користувачів, що вражають уяву. І всі ці дані та аналітичні висновки

стрімголов мчать у США, що ніколи не вирізнялася великим успіхом у сфері захисту персональних даних.

У відповідь на контекстну рекламу у 2002 році Європейський союз приймає Директиву ePrivacy [13]. Вона регламентує використання cookies, що реалізують в тому числі й збір даних для реклами.

Після прийняття цієї директиви, світ сколихає, мабуть, головні сканадли пов'язані з кібербезпекою та даними як вони є. Це стосується і WikiLeaks Джуліана Ассанжа і викриття Едвардом Сноуденом американської програми масового стеження PRISM.

В той же час відбуваються наймасштабніші витоки персональних даних як через хакерські атаки так і через людський фактор. Найбільша їх кількість приходиться на 2010 роки. Яскравим прикладом є витік майже всіх даних з Ashley Madison. Мова йде про канадський сайт знайомств, що був призначений для людей, котрі перебувають у шлюбі. У 2015 році база даних сайту була підвергнута хакерській атаці та вся приватна інформація викладена в мережу. Як результат: величезна хвиля розлучень по всьому світу, декілька випадків суїциду. До того ж, у вільному доступі опинилися дані близько 1 500 користувачів із Саудівської Аравії, де кара за шлюбну зраду сягає смертного вироку. В таких обставинах доволі складно нехтувати значенням захисту персональних даних

На початку весни 2018 року світ сколихнув скандал з витоку персональних даних у найпоширенішій соціальній мережі Facebook. Йдеться про те, як політична компанія Cambridge Analytica зібрала особисту інформацію про 50 мільйонів користувачів Facebook за допомогою додатку, який викрив деталі про особистість людей, соціальні мережі та їх взаємодію на платформі. Незважаючи на ствердження Cambridge Analytica, що він мав інформацію лише про 30 мільйонів користувачів, Facebook визначив, що початкова оцінка була насправді низькою. У квітні компанія повідомила 87 мільйонів користувачів своєї платформи, що їх дані були передані.

Після всіх цих подій, ЄС приходить до висновку про необхідність оновлення вже недієвої Директиви 1995 року. Основна її проблема полягала в тому, що вона напряму не застосовувалася в країнах-членах ЄС. А це в свою чергу призвело до суттєвих відмінностей на рівні національних законодавств. Новий регламент повинен діяти безпосередньо в кожній європейській країні та дозволив би створити

новий підвищений рівень захисту персональних даних на території всього Союзу. Дискусії в цілях прийняття нового закону розпочалися ще в 2012 році, у 2016 р. було опубліковано кінцевий текст регламенту, а 25 травня 2018 року вступив у дію. Його назва – General Data Protection Regulation (далі – GDPR).

Тепер GDPR є найбільш масштабним регуляторним актом із захисту персональних даних на території ЄС. В ньому уточнено поняття персональних даних, наведено розмеження сторін, що співпрацюють з інформацією та передбачено суттєві штрафи за невиконання вимог.

На GDPR законотворча діяльність ЄС у сфері захисту інформації не припинилася. Обробка персональних даних в межах кримінального правосуддя не є периметром дії регламенту, так як потребує встановлення специфічного правового режиму. Тому в 2016 році разом з GDPR була прийнята директива про захист фізичних осіб при автоматизованій обробці персональних даних урядовими органами задля запобігання, розслідування, виявлення і переслідування кримінальних злочинів [14].

Також в цьому ж році приймають директиву NIS [15] (Network and Information Security). Основною метою цього правового акту стає забезпечення високого рівня інформаційної безпеки (ІБ) для операторів критичних інфраструктур та провайдерів цифрових послуг. Мова йде про захист не тільки персональних даних, а про безпеку взагалі будь-яких даних.

Всі ці закони є результатом роботі ЄС у сфері електронних комунікацій, кібербезпеки та приватності даних загалом. Наступним кроком ЄС має бути заміна діючої директиви ePrivacy від 2002 року. Основні питання, які вона має вирішити: метадані (Big Data) та все ті ж cookies. Проект [16] цього регламенту вже був опублікований у 2017 році.

Таким чином GDPR разом з разом з усім вищезгаданим пакетом реформ є результатом майже вікової юридичної думки, заснованої на необхідності захисту приватного життя кожного громадянина в реаліях сьогодення.

Основними складовими законодавства України про інформацію є: Конституція України, законодавчі акти про окремі галузі, види, форми і засоби інформації, міжнародні договори, угоди та стандарти, ратифіковані Україною, принципи і норми міжнародного права.

Фундаментальним законодавчим актом у сфері безпеки інформації є Закон України „Про інформацію” [1], який регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, встановлює основні принципи інформаційних відносин та права громадян на інформацію та їх гарантії.

Важливим також є Закон України „Про захист інформації в інформаційно-телекомунікаційних системах” [2], що регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Також слід згадати Закон України „Про електронні документи та електронний документообіг” [4] оскільки на підприємстві використовуються електронні документи. Дія цього закону поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів.

В області інформаційної безпеки також слід дотримуватись національних стандартів, що відповідають серії міжнародних стандартів представлених такими компаніями як Міжнародна організація зі стандартизації (англ. International Organization for Standardization, ISO) та Міжнародна електротехнічна комісія (англ. International Electrotechnical Commission, IEC). По-перше, це ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою [9]. Він створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ).

Вимоги до захисту в системі інформації, що становить державну таємницю, визначаються [20]. Згідно з [18] державна таємниця (секретна інформація) - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в державних органах, органах місцевого самоврядування, на

підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

Необхідно надавати відповідний гриф секретності рішенням про віднесення інформації до державної таємниці та про скасування цих рішень залежно від важливості їх змісту. Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи зміни до нього у порядку, встановленому цим Законом.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до [1].

Правила, що розглянені у [19] визначають загальні вимоги та організаційні засади забезпечення захисту таємної інформації або інформації, вимога щодо захисту якої встановлена законом:

- відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій;

- усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією;

- модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі;

- під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення;

- доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам;

- у системі здійснюється обов'язкова реєстрація результатів ідентифікації та автентифікації, результатів виконання користувачем операцій з обробки інформації, спроб НСД, фактів надання та позбавлення користувачів права доступу до інформації, результатів перевірки цілісності ЗЗІ. Ідентифікація та автентифікація

користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом;

- передача службової і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними к-аналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного ЗІ;

- у системі здійснюється контроль за цілісністю ПЗ, яке використовується для обробки інформації, програмних та технічних ЗЗІ;

- для забезпечення захисту інформації в системі створюється КСЗІ;

- організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації;

- якщо для створення СЗІ необхідно провести роботи з криптографічного

- захисту інформації, виконавець повинен мати ліцензії на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії;

- захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

По-друге, слід брати до уваги ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки [10].

У сфері захисту персональних даних при використанні хмарних технологій варто спиратися на ISO/IEC 27018:2015 [18]. Він заснований на попередньому стандарті, та містить у собі керівництво із застосування засобів контролю стандарту ISO/IEC 27002, що стосуються персональних даних.

Закон України „Про захист персональних даних” [3] займає своє місце у законодавчій базі інформаційної сфери, оскільки він встановлює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

Також, у сфері національного законодавства слід звернути увагу на такі документи як витяг з Конституції України (стаття 32) [19] про заборону втручання в особисте життя і сімейне життя.

Рішення Конституційного Суду України №2-рп/2012 від 20 січня 2012 року [20] стосується саме роз'яснення попередньої статті й встановлює, чи є збирання, використання і поширення інформації про особу втручанням в її особисте життя.

Конвенція про захист прав людини і основоположних свобод [21] встановила основні права людини, в тому числі ті, що стосуються приватного життя.

Конвенція Ради Європи №108 «Про захист осіб у зв’язку з автоматизованою обробкою персональних даних» [22] узгодила основоположні цінності поваги до недоторканності права людини на особисте життя та безперешкодного обміну інформацією муж народами. До нього можна додати й додатковий протокол до Конвенції Ради Європи №108 «Про захист осіб у зв’язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних» [23].

Закон України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» [24] окрім ратифікації, встановлює уповноваженого з прав людини.

Типовий порядок обробки персональних даних [25] є частиною наказу “Про затвердження документів у сфері захисту персональних даних” та визначає вимоги до обробки персональних даних, порядок їх обробки та ін.

Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних [26] встановлює процедуру здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням вимог законодавства про захист персональних даних.

Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов’язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації [27].

Витяг з Кодексу України про адміністративні правопорушення (стаття 18839 «Порушення законодавства у сфері захисту персональних даних», стаття 18840

«Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини») [].

Витяг з Кримінального кодексу України (стаття 182 «Порушення недоторканності приватного життя») [28], що визначає штрафи та запобіжні заходи.

1.3 Аналіз основних вимог загального регламенту захисту даних

З травня 2018 року Європа перейшла на нові правила обробки персональних даних згідно з регламенту GDPR [17]. Його важливою особливістю є екстериторіальний принцип, тому цьому питанню необхідно приділити увагу й українським компаніям, що орієнтовані на європейський та міжнародний ринок.

GDPR має екстериторіальну дію і застосовується до всіх компаній, що обробляють персональні дані резидентів та громадян ЄС, незалежно від місця розташування такої компанії.

Якщо:

- послуги/товари адаптовані під місцеву мову жителів ЄС;
- послуги/товари сплачуються в місцевих валютах ЄС;
- послуги/товари надаються на національних доменах верхнього рівня країн ЄС (наприклад, “.de”, “.nl”, “.co.uk” та ін.);

компанія має відповідати нормам GDPR.

Також у регламенті розділяються такі поняття як контролер даних (data controller) та процесор даних (data processor). Контролер діє в якості управлінця і несе більшу відповідальність, ніж процесор. Мається на увазі, що контролери вирішують що має відбуватися з персональними даними, та несуть відповідальність за обробку, а процесор несуть функцію виконавця.

Наприклад, хмарна система, якою користуються співробітники для виконання процесів та задач і де зберігаються персональні дані ваших клієнтів є процесором, а контролер — володілець системи.

Персональні дані (згідно GDPR) — це будь-яка інформація, що стосується ідентифікованої фізичної особи (суб'єкту даних), за якою прямо чи опосередковано можна її визначити. До такої інформації відносяться: прізвище та ім'я, адреса електронної пошти, дані про місце розташування, онлайн ідентифікатор або один чи

декілька факторів, характерних для генетичної, фізичної, фізіологічної, економічної, розумової, соціальної, культурної ідентичності цієї фізичної особи (п. 1 ст. 4). Це доволі широке визначення, під нього підпадають навіть IP-адреси.

Також слід відзначити, що існують певні типи персональних даних, що відносяться до категорії особливих або конфіденційних персональних даних. Це інформація, що викриває: етнічну або расову приналежність, політичні погляди, релігійні чи філософські переконання, членство і профспілках. Крім цього, до такої інформації відносяться генетичні, біометричні дані, що використовуються для ідентифікації фізичної особи, дані про стан здоров'я, відомості, що стосуються сексуального життя чи сексуальної орієнтації (п. 9).

Основні принципи обробки персональних даних:

1. Законність, справедливість та прозорість. Персональні дані повинні оброблятися законно, справедливо та прозоро. Будь-яку інформацію, що стосується мети, методів та об'ємів обробки персональних даних слід викладати максимально доступно та просто.
2. Обмеження мети. Дані повинні збиратися та використовуватися винятково заради заявленної компанією мети.
3. Мінімізація даних. Не можна збирати дані в більшому об'ємі, що суперечить меті обробки.
4. Точність. Особисті дані, що є неточними повинні бути видалені або виправлені (за запитом користувача).
5. Обмеженість зберігання. Особисті дані повинні зберігатися способом, що дозволяє ідентифікувати суб'єкта даних на строк, що не перевищує необхідного для мети обробки.
6. Цілісність та конфіденційність. Під час обробки даних користувача компанії необхідно забезпечити захист персональних даних від несанкціонованої або незаконної обробки, знищення чи пошкодження.

Компанії зобов'язані повідомляти наглядові органи про (а в деяких випадках і суб'єктів даних) про порушення, що пов'язані з персональним даними не пізніше ніж 72 години після виявлення такого порушення.

GDPR значно розширює права громадян та резидентів ЄС з контролю за персональними даними. Європейські користувачі мають право на запит

підтвердження факту обробки їх даних, місця та мети обробки, категорії оброблюваних даних, яким третім особам ці дані доступні, період, протягом якого дані будуть оброблятися, на джерело отримання організацією персональних даних і вимагати їх виправлення. Також користувач має право вимагати припинення обробки персональних даних.

У GDPR також передбачено право на забуття. Воно надає європейцям можливість видаляти свої дані за запитом для того, щоб уникнути їх розповсюдження або передачу третім особам. Будь-яка компанія, що обробляє дані, зобов'язана видаляти персональні дані за запитом володільця, якщо це не суперечить інтересам суспільства або іншим фундаментальним правам європейців.

Право на переносимість даних є новацією в правилах обробки даних, введених з GDPR. Сутність полягає в тому, що компанія зобов'язана надавати електронну копію персональних даних іншій компанії за запитом суб'єкту даних.

GDPR встановлює високі вимоги щодо з приводи форми отримання згоди на обробку персональних даних. Згода людини на обробку персональних даних повинна бути виражена у формі ствердження або у формі активних дій користувача. Згода буде недійсною, якщо у користувача не було вибору або не було можливості відмінити свою згоду без збитку для себе. Якщо користувач дав згоду, то контролер повинен мати змогу продемонструвати це.

Дитячі персональні дані потребують особливого захисту, оскільки вони менш обізнані про ризики, наслідки, гарантії та права у відношенні обробки персональних даних. Згода на обробку персональних даних дитини повинно бути авторизовано батьками. Вік встановлює кожна країна ЄС (від 13 до 16 років).

Необхідність призначення відповідального за захист персональних даних стосується компаній, що регулярно та систематично проводять масштабні спостереження або які здійснюють масштабну обробку персональних даних (медичні записи або відомості про кримінальну судимість)

1.4 Постановка задачі

Проведений аналіз однозначно вказує на необхідність розробки рекомендацій з впровадження GDPR в Україні, а саме у сфері хмарних технологій. Оскільки цієї сфери регламент торкнеться вперше.

Для розробки таких рекомендацій потрібно виконати наступні задачі:

- визначити особливості впровадження регламенту при використанні хмарних технологій;
- сформувати етапи підготовки до впровадження вимог GDPR у SaaS-моделі;
- провести аналіз інформаційних ризиків;
- розробити шаблони для впровадження GDPR у сфері хмарних технологій.

Висновки до першого розділу

У цьому розділі було проведено дослідження принципів хмарного обчислення даних та виділено три основні моделі обслуговування. Був проведений аналіз поточної ситуації в Україні в галузі безпеки персональних. Наведені приклади найбільших випадків кіберзлочинів за останній період.

Обґрунтовано актуальність проблеми захисту персональних даних у світовому масштабі при аналізі розвитку нормативної бази Європейського союзу з огляду на історичні події локального та глобального масштабів. Наведені ключові моменти розвитку законотворення у сфері захисту персональних даних.

Було проведено аналіз основних вимог загального регламенту захисту даних, визначено його особливості.

Розглянуто нормативно-правову базу у сфері захисту інформації. Виділені основні закони, нормативні документи та державні стандарти, що стосуються розробки політики безпеки інформації на підприємстві.

Сформовано задачі, які відображають перелік робіт, що передують впровадженню вимог Загального регламенту захисту даних (GDPR) в разі використання хмарних технологій.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Основні етапи підготовки до впровадження вимог GDPR у SaaS-моделі

Програмне забезпечення як послуга (SaaS) – це найбільш розповсюджена форма доставки онлайн-додатків користувачам. Це дуже успішна бізнес-модель, але тут доволі часто виникає плутанина, особливо, коли справа стосується конфіденційності та дотримання нормативних вимог.

Раніше програмне забезпечення купувалося напряму, в цифровій чи матеріальній формі та завантажувалося безпосередньо на пристрій. Із збільшенням хмарних обчислень для розробників програм стало більш популярним замість цього створювати хмарний сервіс та брати з користувачів абонентську плату за використання цього сервісу.

Ця нова бізнес-модель дозволила клієнтам отримувати доступ до послуги через різноманітні пристрої, а не через виділене. Це також мінімізувало накладні витрати компаній, бо усунуло необхідність встановлення та обслуговування обладнання на місці.

Абонентська плата (зазвичай щомісячна) допомагає клієнтам краще планувати свої витрати, а також самостійно обирати, які функції та послуги їм потрібні.

Окрім цього, можливість просто завантажувати та застосовувати будь-які оновлення служб, замість покупки нового програмного забезпечення, зробило користування ПЗ більш зручним.

Проте ці переваги також створили ряд нових проблем, з якими можна зіштовхнутися як користувачі SaaS, так і розробники. Особливо, коли йдеться про безпеку та конфіденційність.

Основна проблема безпеки у використанні ПЗ в мережі Інтернет — як і споживачів, так і для компаній — пов'язана з довірою, що потребується з усіх сторін.

Як бізнес, що використовує SaaS, ви довіряєте сторонньому постачальнику всі свої бізнес-процеси, конфіденційні дані клієнтів та компаній та іншу важливу інформацію.

Як володілець бізнесу та клієнт SaaS, ви так само можете контролювати послуги, що використовуєте та дані, що збираєте. Тому важливо бути в курсі всіх необхідних законів про конфіденційність, для забезпечення належного рівня безпеки даних, що збираєте у клієнтів.

Розглянемо ключові розділи GDPR в розрізі їх застосування в SaaS-моделі.

Збільшення території дії. GDPR розширила сферу своєї діяльності, долучивши міжнародні компанії, які збирають дані будь-яко громадянина в будь-якій країні-члені ЄС. Це збільшення торкнеться організацій, що засновані в ЄС, а також організації в інших країнах, що пропонують свої продукти та/або послуги громадянам ЄС.

Великі штрафи за невиконання.Якщо буде встановлено, що компанія не слідує GDPR, встановлюються штрафи, що сягають 20 мільйонів євро або 4% від загального обігу компанії (в залежності від того, яка сума більша).

Цих величезних штрафів можна уникнути, якщо буди песним, що ваша платформа SaaS відповідає всім нормам GDPR.

Явна згода користувачів. Це, напевно, є чи не найважливішою частиною GDPR. Мова йде по згода, яка необхідна компаніям від їх суб'єктів даних до того, як відбудеться будь-який збір чи обробка даних.

Враховуючи те, що метою GDPR є забезпечення споживачам якомога високий рівень контролю над їх особистою інформацією, явна згода є чудовим способом реалізації.

Умови для отримання згоди стали більш жорсткими, і тепер компанії зобов'язані викласти свій запит на отримання згоди, використовуючи чіткі та стислі терміни, що зрозумілі для кожного відвідувача сайту чи користувача.

Ось приклад, як Dropbox отримує згоду під час безкоштовної пробної версії чи реєстрації аккаунту, коли він отримує персональні дані від людей. Після запиту іншої особистої інформації, такої як прізвище, ім'я, адреса електронної пошти й фінансової інформації, користувач повинен активувати поле “Я згоден з Бізнес-угодою та умовами Dropbox”.

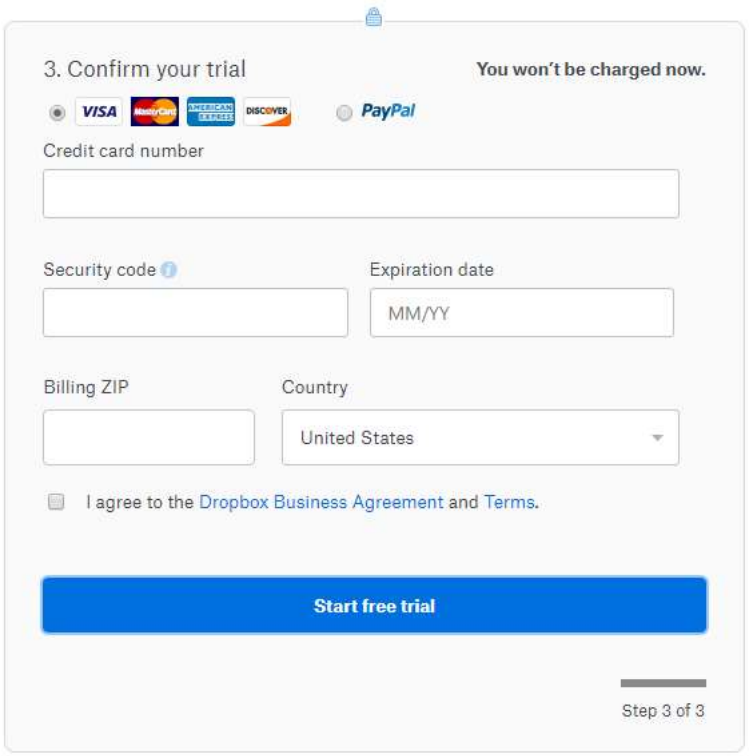

Рис. 2.1 — Згода на обробку ПД на прикладі сервісу Dropbox

Це гарний приклад згоди, оскільки чітко ясно, з чим користувач погоджується, коли поле активне і для початку пробної версії необхідно це зробити.

Повідомлення про порушення. Якщо будь-яке порушення сталося по відношенню до даних компанії, це порушення повинно бути доведене до відома наглядових органів протягом 72 годин після виявлення порушення. Клієнти також мають бути повідомлені протягом того ж часу.

Будь-які порушення повинні бути виявлені процесорами даних, що діють від імені вашої компанії та повідомлені контролерам даних вашої компанії. Ці порушення завжди повинні заноситися до внутрішнього реєстру, аби відслідковувати події.

На Рис. 2.2 наведено основні складові процесу сповіщення у разі витоку персональних даних.

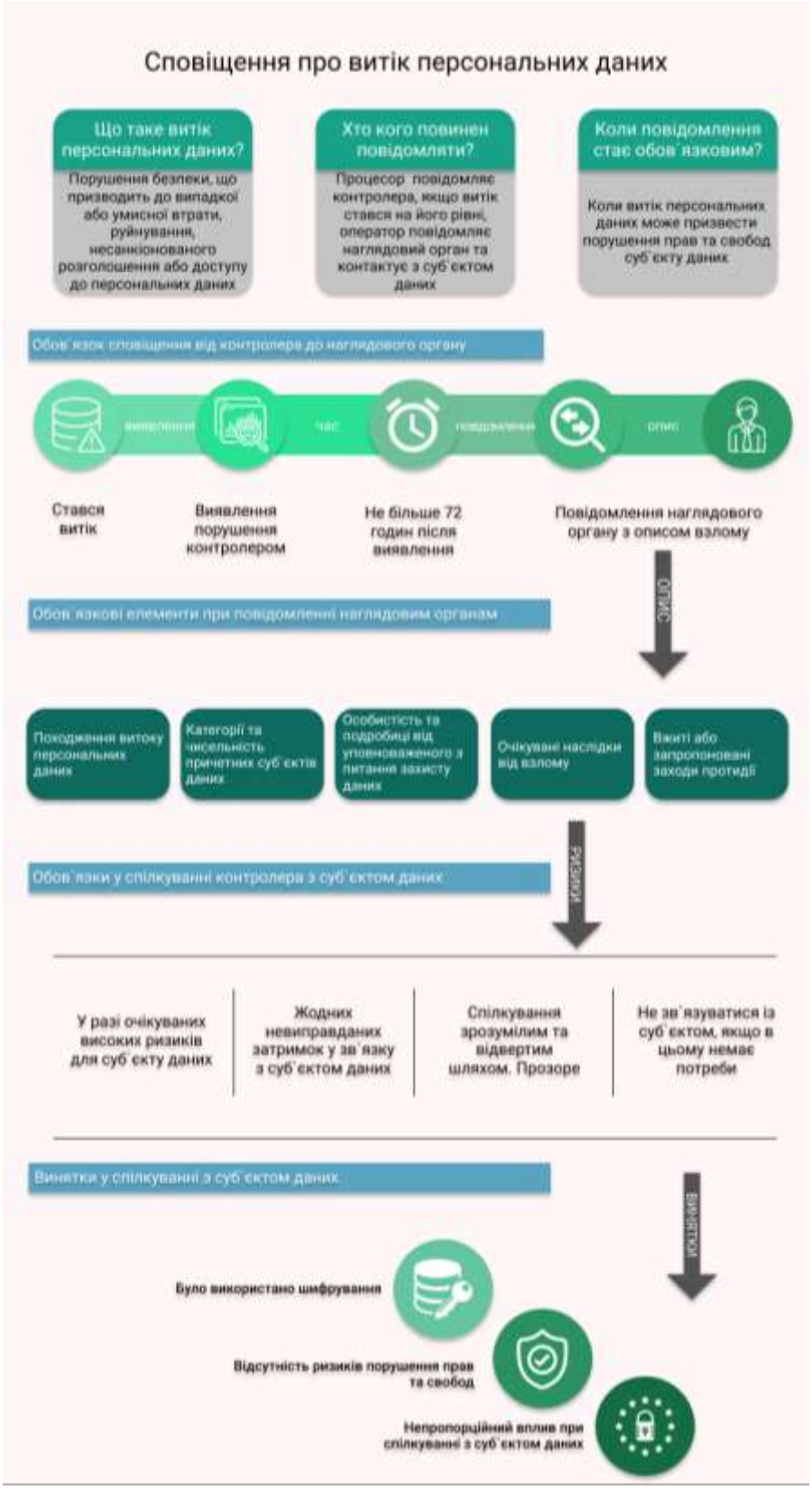

Рисунок 2.2 — основні складові процесу сповіщення у разі витоку персональних даних

Право на доступ. GDPR надав користувачам право на отримання власної інформації, яку вони передали контролеру даних. Цей доступ повинен бути наданий простим способом, безкоштовно та в електронному форматі.

Надання доступу до власних даних — це чудовий спосіб розширити можливості клієнтів, зняти будь-які питання, що вони можуть мати стосовно їх конфіденційності та впевнитися, що ваша компанія залишається цілком чесною та прозорою.

Доступ до таких даних необхідно надати протягом 4 тижнів.

Право на забуття. Це право дозволяю клієнтам робити на запит на видалення всіх їх даних, які колись було зібрані компанією. Якщо цей запит відправлений, це означає, що все сторонні сервіси також мають припинити обробку персональних даних цього клієнта.

Не дивлячись на те, що вже існують умови, що стосуються права на видалення, такі як нерелевантні дані, або відмова клієнта від згоди на обробку ПД, цей додаток є гарним способом підвищити лояльність клієнтів та відвідувачів сайту.

Співробітники з захисту інформації. Окрім процесорів та контролерів даних, є інша не менш важлива роль, пов'язана з дотримання норм GDPR, - це співробітник з захисту даних (Data Protection Officer, DPO). Ця посада необхідна не в усіх випадках, але якщо вам потрібен такий співробітник, то на цю посаду повинна бути призначена особа, що має відповідні знання про закони та практики з захисту даних, або зовнішній службі, яка може надати належні рекомендації та підтримку.

DPO повинен допомагати компанії в підтримці GDPR та іншим пов'язаним законам, вони несуть особливий рівень відповідальності та звітності.

Також вони зобов'язані навчати співробітників компанії всіх необхідних вимог GDPR, а також виступати у ролі контактної особи між компанією та наглядовими органами.

Проведення оцінки впливу на захист даних. Якщо у вашому бізнесі обробка окремих персональних даних може призвести до високих ризиків для свободи та конфіденційності цих осіб, вам знадобиться провести так звану оцінку впливу на захист даних (Data Protection Impact Assesment, DPIA).

DPIA проводиться спеціалістом із захисту даних, його метою є надання допомоги у виявленні основних сфер ризику в вашій роботі.

Головним питанням залишається визначення ролей: контролер чи процесор даних. Особливістю бізнесу SaaS є те, що технічно він може бути і контролером і процесором даних. Це пов'язано з тим, що платформа SaaS – це об'єкт, котрий збирає персональні дані користувачів і приймає рішення про призначення цього збору.

Платформи SaaS також підтримують контроль будь-яких зібраних даних та можуть вирішувати, яким чином ці дані обробляються.

Приклади GDPR-сумісних та несумісних SaaS-платформ.

Shufti Pto, європейський стартап, демонструє чудовий приклад відповідності вимогам GDPR на своєму сайті. Як видно нижче, замість того, щоб ховати згадку про відповідність GDPR в своїй Політиці конфіденційності, вся сторінка присвячена поясненню того, як компанія виконує вимоги GDPR.

Рисунок 2.3 — Приклад сайту, що відповідає GDPR

У цьому керівництві розглядаються такі теми, як файли cookie, законні засади, видалення, доступ до даних користувача, індивідуальні запити прав користувача та ін.

Використовуючи мову, що легко читається та уникає будь-яких технічних термінів, компанія гарантує, що кожен зможе прочитати Політику відповідності та зрозуміти її.

Пряме посилання на Політику відповідності включена у фіксований нижній колонтитул сайту, тому користувачам напрочуд легко його знайти.

Прикладом невідповідності може слугувати SaaS-платформа ToutApp.

Хоча це й американська компанія, ймовірно вона збирає дані про іноземних користувачів. Проте, їх Політика конфіденційності не містить жодної інформації про

це законодавство. Вона охоплює значний спектр важливої інформації, але востаннє була змінена до впровадження GDPR і може враховуватися як несумісна з GDPR.

Компанія Picksaas спитала 30 власників бізнесу, що підпадає вимогам GDPR, що було найскладнішим у впровадженні GDPR у ваш бізнес. Відповіді далі наведені у порядку зменшення.

1. Модифікація Політики конфіденційності.
2. Підпис згоди про обробку персональних даних з усіма процесорами даних.
3. Налагоджувальні етапи в середині компанії.
4. Постачання згоди про обробку персональних даних до користувачів.
5. Технологічні зміни продукту.
6. Призначення співробітника із захисту даних.

Не дивлячись на те, що GDPR спершу може здатися вкрай заплутаним з багатьма різними аспектами, котрі необхідно брати до уваги, краще розглядати відповідність як інвестицію, а не як неприємність, яку необхудно подолати.

Ваша SaaS-платформа може досягнути повної відповідності GDPR, якщо ви:

- оновите свою Політику конфіденційності, для деталізування дії з персональними даними, а також усіх прав користувачів;

- зробите запит на явну згоду ваших користувачів на обробку ПД перед збором та обробкою будь-яких даних;

- зрозумієте обов'язки контролерів та процесорів даних і забезпечите належне виконання обох ролей.

2.2 Аналіз інформаційних ризиків

Отже, у вашої компанії є певний набір даних клієнтів, де ви зберігаєте всі особисті дані, включно з контактною інформацією, переліком покупок, рахунків і т.д.

Незалежно від того, хто ви — процесор чи контролер даних, ви зобов'язані захистити дані клієнта згідно установ GDPR, оскільки ці дані є персональними.

Для злагодженої роботи вашої організації цей набір даних повинен бути доступний для багатьох ваших співробітників, з різних пристроїв, також може знадобитися можливість сумісної роботи та обміну даними один з одним. Зазвичай, саме в такий час у гру вступають локальні сховища або інші хмарні рішення.

Для захисту персональних даних GDPR виділяє декілька технічних заходів, одним із них є шифрування. Зрозуміло, що існує багато різних способів шифрування.

Який з підходів забезпечує до зберігання та шифрування даних забезпечує найкращий захист і ефективний у найбільш розповсюджених сценаріях атак? Відповідь на це питання залежить від того, наскільки реальним є сценарій ідентифікування особи з зашифрованого набору даних у разі витоку цих даних. Тобто, потрібно дослідити, можливість того, що збережені зашифровані персональні дані залишаються такими, що читаються, зрозумілими даними, які можна використати для ідентифікації власника.

Розглянемо три основні підходи до захисту персональних даних за допомогою шифрування:

1. Локальне збереження зашифрованих даних. Ви шифруєте дані і самостійно зберігаєте їх локально на власних серверах.
2. Хмарне сховище з серверним та транзитним шифруванням. Ви довіряєте шифрування даних хмарному провайдеру, він шифрує ці дані і зберігає їх у себе разом з відповідними ключами шифрування та дешифрування. В цьому випадку провайдер зможе їх розшифрувати за вашим запитом. Такі послуги пропонуються майже всіма хмарними провайдерами, наприклад Google, Dropbox, Amazon.
3. Хмарне сховище з наскрізним шифруванням на стороні клієнта. Ви шифруєте дані на власній стороні, а у сховищі зберігаєте вже зашифровані масиви даних. Таким чином ви єдиний, хто може отримати доступ до ключа шифрування.

Мета GDPR – захистити людей від розкриття їх особистих даних. Відповідно до GDPR, персональні дані — це будь яка інформація, що відноситься до ідентифікованої особи. Раніше було описано, що визначення персональних даних залежить від контексту і в кінцевому випадку потребує перевірки того, хто має можливість отримати доступ до даних і чи має він/вона можливість зв'язати ці дані з якоюсь особою. Згідно запропонованих вище сценаріїв, це означає, що зашифровані дані є персональними, якщо будь-який вірогідний зловмисник, ким би він не був, має реальний шанс з'ясувати особистість суб'єктів даних (що шифруються). Загалом достовірність залежить від мотивації зловмисника (наприклад, його стимулів чи

стримуючих факторів для повторної ідентифікації будь-якого суб'єкту даних), а вірогідність успіху залежить від технічної складності атаки (на скільки легко отримати дешифрований набір даних). Мотивація та вірогідність успіху не є цілковито незалежними. Чим легше атака, ти більше мотивації може бути у зловмисника, але на даний момент ми не враховуємо цю залежність.

Для того, щоб зрозуміти всі переваги та недоліки кожного з підходів до шифрування, слід розібрати правдоподібнсть та вірогідність успіху деяких атак, що спрямовані на повторну ідентифікацію будь-якої особи, дані якої зашифровані одним із вищезгаданих способів.

1. Локальне збереження зашифрованих даних.

Це рішенні доволі просте та безпечне лише в тому випадку, якщо ваш сервер, на якому може зберігатися ключ дешифрування або термінал, що може бути використаний для представлення кодової фрази для відновлення ключа добре захищені. Однак, забезпечити належний рівень безпеки набагато складніше, аніж може здатися на перший погляд. Брандмауерів, антивірусних програми чи інших стандартних продуктів безпеки зазвичай недостатньо. Складні направлені атаки спроможні обійти навіть основні засоби безпеки, використовуючи фішинг чи соціальну інженерію для встановлення шкідливих програм у вашу систему. Наприклад, це може статися, коли один з ваших співробітників відкриє невинний додаток або перейде за посиланням в електронному листі, підробленому зловмисником. Шкідливі програми, вставлені на будь-який комп'ютер у вашій локальній мережі, здатні використовувати вразливості нульового дня в певних програмних компонентах вашої системи, для того щоб отримати доступ до конфіденційних файлів, що можуть містити в собі ключ для дешифрування даних. Окрім того, такі програмі можуть навіть реєструвати натискання клавіш при вводі кодової фрази для дешифрування набору даних. Компанії, що вкладають чималі кошти в безпеку чутливі для таких загроз.

2. Хмарне сховище з серверним або транзитним шифруванням

Тепер розглянемо, що станеться в разі завантаження ваших не зашифрованих даних клієнтів до постачальника хмарних послуг, котрий буде шифрувати цей набір і буде зберігати його разом з ключем шифрування та дешифрування у безпечному місці. Кожного разу, коли вам знадобляться ці дані, постачальник їх дешифрує і

відправляю вже в дешифрованому вигляді захищеним каналом. Наскільки легко повторно ідентифікувати особи, якщо стався витік? Чи можуть зашифровані дані бути персональними?

Знову ж, це залежить від того, наскільки легко зловмисник, ким бі він не був, може отримати доступ до дешифрованих даних клієнта. Для зовнішнього зловмисника (хакера), отримання доступу до серверу провайдера може біти більш технічно складним, аніж у попередньому випадку, де ви самостійно зберігали дані. Причина в тому, що хмарні провайдери зазвичай набагато більше підготовлені до таких атак. Проте, вірогідність такої атаки не є незначною. Значна різниця відчувається в мотивації зловмисника: він розуміє, зо провайдер зберігає ключі до даних не тільки ваших клієнтів, і тому в нього може бути набагато більше причин атакувати саме провайдера.

До того ж, потенційні (внутрішні) зловмисники включають й самого постачальника разом з його співробітниками, котрі легко можуть отримати ваш ключ дешифрування. Зрозуміло, що у самого постачальника навряд буде стимул до відстеження ваших клієнтів через юридичні наслідки та втрату репутації, але розчарований чи матеріально мотивований співробітник цілком може це зробити.

3. Хмарне сховище з наскрізним шифруванням на стороні клієнта

Це рішення цілковито об'єднує переваги попередніх підходів; тільки ви знаєте ключ дешифрування, але дані надійно зберігаються у провайдера. Припустимо, що в найгіршому випадку зловмисник якимось чином отримав копію зашифрованих даних клієнта.

Тепер, чи може зловмисник пов'язати ці дані з одним з ваших клієнтів. В теорії, це неможливо. Оскільки зашифровані дані можуть бути пов'язані з певним клієнтом тільки в тому випадку, якщо вони успішно дешифровані. Теоретично це можливо лише в тому випадку, якщо зловмисник просто вгадає ключ дешифрування. В реальному стані в жодного зловмисника не буде розумного шансу вгадати ваш ключ, а це в свою чергу означає, що зашифровані дані про ваших клієнтах розглядаються як ті, що не підлягають інтерпретації, цілковито випадкові “сміттєві” дані для тих, хто не має ключа. Тому, поки дані не дешифровані, їх витік є безпечним для суб'єктів даних.

Однак, світ далекий від ідеалу. По-перше, ваш ключ генерується з кодової фрази або пароля. Якщо його легко вгадати, зловмисник може дешифрувати дані ваших клієнтів. Якщо у зловмисника є вірогідний шанс вгадати кодову фразу, використовуючи, наприклад, шкідливе ПЗ, що реєструє натискання клавіш, як в підході 1, тоді зашифровані дані можна розглядати як персональні; у випадку витоку вони можуть бути повторно ідентифіковані. В свою чергу це означає, що обережність не завадить, аби звести нанівець хоча б ризики атак методом перебору, потрібно використовувати надійні паролі, що генеруються унікально для кожної служби, якою ви користуєтеся.

По-друге, сам алгоритм шифрування, що використовується вами або вашим провайдером може бути вразливим до певних видів атак. Це, до речі, може відноситися до всіх трьох розглянутих підходів. Наприклад, зловмисник може використати деякі недоліки проекту в схемі шифрування. Це досить малоймовірний варіант, особливо якщо ваш провайдер використовує стандартизовані схеми шифрування. Другий і більш ймовірний спосіб взлому схем шифрування — використання недоліків реалізації в деяких програмних компонентах, що використовуються у схемі шифрування. Ці недоліки можуть бути умисно бути в коді, наприклад, за вимогою уряду. Проте, це малоймовірно, якщо провайдер використавує реалізації з відкритим вихідним кодом та прозорий в своїх операціях і в тому, як вони керують урядовими запитами. Однак, використання не навмисних недоліків реалізації (наприклад, типове переповнення буфера) набагато ймовірніше. Дійсно, недоліки реалізації неминучі, доки програмне забезпечення розробляють люди. Найкраще, що можете зробити ви з вашим провайдером, - це використовувати стандартизовані алгоритми та бути максимально прозорими, та регулярно оновляти програмні компоненті.

Зрозуміло, що найбільш безпрограшний варіант — це використання третього підходу. Нижче в таблиці відображено стислий виклад вищенаведеного аналізу того, яка вірогідність успіху двох розглянутих зловмисників, а саме провайдера хмарних обчислювань (або його співробітників) і зовнішнього зловмисника. Оцінюємо ймовірність та вірогідність успіху найбільш масштабної атаки в кожному випадку. Мотивацію та вірогідність успіху оцінюємо по шкалі з чотирьох значень вірогідності: низький, середній, значний та великий. Наприклад, якщо якась з атак

має ґрунтовну вірогідність статися і бути успішною, тоді вона має велику чи значну мотивацію і вірогідність успіху. В цьому випадку зашифровані дані можуть перетворитися на персональні, оскільки при потраплянні до чужих рук можуть бути повторно ідентифіковані.

З таблиці та проведеного аналізу випливає, що хмарне збереження з наскрізним шифруванням на стороні клієнта - це варіант, де зашифровані дані клієнта з меншою вірогідністю будуть розглядатися як персональні та використовуватися для повторної ідентифікації суб'єктів даних. Тому що, у провайдера не має грунтовних засобів для доступу до ключу дешифрування, а зовнішній зловмисник менше мотивований, порівнюючи з випадком, коли провайдер зберігає ключі

Табл. 2.1 — Аналіз ризиків

		Зловмисник			
		Внутрішній		Зовнішній	
		Мотивація	Вірогідність успіху	Мотивація	Вірогідність успіху
Підхід	1. Локальне збереження зашифрованих даних	Низька	Низька	Середня	Значна
	2. Хмарне сховище з серверним або транзитним шифруванням	Середня	Велика	Велика	Середня
	3. Хмарне сховище з наскрізним шифруванням	Низька	Низька	Середня	Середня

Ще одна вагома причина обрати хмарне збереження замість локального — у хмарі набагато менше шансів втрати даних. Це підвищує доступність і цілісність ваших даних, що також є явним принципом захисту інформації в GDPR.

2.5 Розробка рекомендації щодо впровадження загального регламенту захисту даних

На основі попередніх досліджень, очевидним стає факт у необхідності розробки рекомендації щодо впровадження GDPR. Вони мають бути універсальними і змістовними, оскільки це зменшить час на впровадження та відповідність вимогам GDPR.

Реалізація GDPR в кожній компанії може бути різною. Але є певний перелік кроків і рекомендацій, що є критичними.

Після того, як ви визначилися із застосування GDPR до вашої організації необхідно:

1. Визначіться, ким ви є: контролером чи процесором даних? Від цього буде залежати сфера вашої відповідальності.

2. Створіть перелік даних, які ви збираєте у ваших користувачів. Для цього можна створити таблицю, в якій необхідно перелічити типи даних, які ви збираєте в своїй компанії, в тому числі: джерело даних, кому ці дані можуть бути надані, мету збору, термін зберігання. Цю таблицю можна зробити відкритою, це також дозволяє бути максимально відкритими з вашими користувачами.

3. Створіть список ваших баз даних, де буде інформація про те, як ці дані передаються один між одним.

4. Створіть список усіх задіяних процесорів даних (зазвичай програмне забезпечення SaaS) та підпишіть згоду про обробку даних (Data Processing Agreement, DPA). Окрім цього, необхідно визначити, чи обробляють вони персональні дані.

5. Оновіть вашу Політику конфіденційності. Необхідно додати наступні елементи: як ви збираєте ПД; як ви використовуєте зібрані дані; перелік сторін, з якими ви ділитеся даними; адреса електронної пошти, до якої користувачі можуть звернутися в разі бажання отримати доступ чи видалити свої персональні дані; адреса електронної пошти співробітника з захисту даних. Нова політика повинна бути максимально прозорою. Перелічіть всі місця, де ви зберігаєте дані.

6. Оновіть політику використання файлів cookie. Окрім інформації про тип файлів cookie, які ви використовуєте, вам необхідно вказати інформацію про причину використання цих файлів на вашому сайті.

7. Назначте співробітника з захисту даних.

8. Відправте електронний лист вашим співробітникам про те, як ви виконуєте GDPR. Якщо у вас невелика компанія, доцільним є проведення невеликої зустрічі. Якщо ви є процесором даних, необхідно організувати навчання для ваших співробітників.

9. Перевірте відповідність технічної безпеки. Якщо ви є технічною компанією (наприклад, SaaS), краще бути певним, що продукт технічно захищений, оскільки будь-який виток може призвести до значних штрафів.

10. Створіть схему відповіді для користувачів, як бажають отримати доступ до своїх даних. Згідно з новими стандартами GDPR ваші користувачі, клієнти і партнери завжди можуть: робити запит на доступ до їх даних для передачі їм або третім особам; оновити свої ПД в вашій базі даних; видалити свої ПД; заборонити продовжувати обробку. Вірогідно, в перші роки існування GDPR таких запитів буде багато. Тому слід налагодити пов'язані з цим комунікації.

11. Додайте поле “прийняти” до кожної форми збору даних. Ви повинні бути певні в тому, що відвідувачі приймають вашу оновлену Політику конфіденційності. Це повинно відбуватися в той момент, як користувач залишає будь-яку особисту інформацію на сайті. В рамках GDPR тепер неможливо встановити згоду за змовчуванням. Крім того, якщо ви проводите якісь маркетингові кампанії по електронній пошті, перевірте, аби там також була форма відписки.

12. Встановіть процеси в середині компанії, котрі забезпечать виконання прав ваших користувачів.

13. Якщо вам непотрібно зберігати деякі особисті дані, просто видаліть їх. Наприклад, якщо у вас залишився застарілий перелік розсилки. Окрім цього, ви маєте бути певні, що дані ваших клієнтів видаляються з баз даних усіх ваших процесорів даних.

Зараз існує багато шуму з приводу GDPR. З одного боку це цілковито виправдано, але з іншого, GDPR – це перш за все прозорість, справедливість та серйозність по відношенню до ваших клієнтів та партнерів.

Зберігайте ваші дані у безпеці та будьте певні, що ви серйозно ставитеся до всіх запитів клієнтів. Внесіть необхідні зміни до документації на вашому сайті. Тоді GDPR не буде вадою для вашого бізнесу.

Висновки до другого розділу

У цьому розділі було визначено основні етапи впровадження вимог загального регламенту захисту даних на прикладі однієї з трьох основних моделей обчислення хмарних технологій — SaaS. Визначено особливості цього методу.

Було розглянуто три способи збереження даних з різними видами шифрування. Відповідно до них було проведено аналіз інформаційних ризиків та визначено оптимальній спосіб збереження даних.

Розроблено рекомендації щодо впровадження загального регламенту захисту даних, дотримуючись попередніх досліджень.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Вступ

Метою даного розділу є обґрунтування економічної доцільності застосування рекомендацій щодо впровадження GDPR на підприємствах поштового зв'язку України.

Для визначення ефективності необхідно розрахувати:

1. Капітальні витрати на розробку, впровадження та підтримку рекомендацій;
2. Трудомісткість витрати на розробку, впровадження та підтримку рекомендацій;
3. Річні експлуатаційні витрати на впровадження та підтримку рекомендацій;
4. Показники економічної ефективності застосування рекомендацій в організації.

3.2 Визначення трудомісткості розробки та опрацювання програмного продукту

Нормування праці в процесі створення рекомендацій істотно ускладнено через творчій характер праці програмістів. Проте трудомісткість розробки і опрацювання ПЗ може бути розрахована на основі системи моделей з певною точністю оцінки.

Трудомісткість створення ПЗ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного програміста):

$$t = t_{тз} + t_в + t_а + t_{пр} + t_{опр} + t_6 \text{ , годин,} \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_в$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_а$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання програми на ПК;

t_6 – тривалість підготовки технічної документації на ПЗ.

Підрахуємо трудомісткість:

$t_{тз}$ = 13 годин;

$t_в$ = 23 години;

$t_а$ = 6 годин;

$t_{пр}$ – 8 годин;

$t_{опр}$ – 2 години;

t_6 – 4 години.

Використовуючи формулу (3.1) обчислюємо трудомісткість створення ПЗ:

$$t = 14 + 22 + 6 + 8 + 2 + 4 = 56 \text{ годин}$$

Витрати на створення програмного продукту $К_{пз}$ складаються з витрат на заробітну плату виконавця програмного забезпечення $З_{зп}$ і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК $З_{мч}$:

$$К_{пз} = З_{зп} + З_{мч}, \text{ тис. грн.} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \text{ x } З_{пр}, \text{ грн,} \quad (3.3)$$

де t – загальна тривалість створення ПЗ, годин;

$з_{пр}$ – средньогодинна заробітна плата спеціаліста з нарахуваннями, грн/годину.

Використовуючи формулу (3.3) обчислюємо заробітну плату виконавця:

$$З_{зп} = 56 \text{ x } 141 = 7896 \text{ , грн.}$$

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \text{ x } С_{мч} + t_6, \text{ грн,} \quad (3.4)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

t_6 – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \times t_{нал} \times С_е + (Ф_{зал} \times Н_а) / F_р + (К_{лпз} \times Н_{апз}) / F_р \text{ , грн,} \quad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$t_{нал}$ – кількість ПК;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р = 1920$).

Використовуючи формулу (3.5) обчислюємо вартість 1 години машинного часу ПК:

$$С_{мч} = 0,2 \times 2 \times 1,67 + (4000 \times 0,5) / 1920 + (5000 \times 0,25) / 1920 = 2,36 \text{ грн.}$$

Використовуючи формулу (3.4) обчислюємо вартість машинного часу для налагодження програми на ПК:

$$З_{мч} = 5 \times 2,36 + 4 = 15,8 \text{ грн.}$$

Використовуючи формулу (3.2) обчислюємо витрати на створення програмного продукту:

$$К_{пз} = 7896 + 15,8 = 7911,8 \text{ грн.}$$

3.3 Розрахунок капітальних (фіксованих) витрат

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \text{ грн.} \quad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн (2000 грн вартість розробки проекту та 3000 грн вартість послуг залучених зовнішніх консультантів);

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн (Windows 10 Pro — 3000 грн на рік, антивірус 360 Total Security — 900 грн ліцензія на рік, Visual Studio та Microsoft Office — 1100 грн);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн (для проекту ну потребується створення ПЗ);

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн (твердотільний диск SSD 128 GB — 1200 грн);

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн (послуги навчання персоналу — 1000 грн);

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн (послуги спеціаліста зі встановлення обладнання — 1200 грн).

Використовуючи формулу (3.6) обчислюємо витрати на капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки:

$$К = 5000 + 5000 + 0 + 1200 + 1000 + 1200 = 13400 \text{ грн.}$$

3.4 Розрахунок експлуатаційних (поточних)

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ тис. грн.} \quad (3.7)$$

де $С_в$ – витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки (20% від капітальних витрат);

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки (46% від капітальних витрат);

$С_к$ – керування системою інформаційної безпеки, визначається за формулою:

$$С_к = С_{ел} + С_{тос} \quad (3.8)$$

де $С_{ел}$ – Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року;

$С_{тос}$ – Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки;

$С_{ел}$ визначається за формулою:

$$С_{ел} = Р \text{ x } F_р \text{ x } Ц_е \text{ , грн} \quad (3.9)$$

Використовуючи формулу (3.9) обчислюємо вартість електроенергії, що споживається апаратурою системи інформаційної безпеки протягом року:

$$С_{ел} = 0,2 \text{ x } 1920 \text{ x } 1,67 = 641,28 \text{ грн.}$$

Використовуючи формулу (3.8) обчислюємо витрати на керування системою інформаційної безпеки $С_к$:

$$С_к = 641,28 + (13400 \text{ x } 0,02) = 909,28 \text{ грн.}$$

Використовуючи формулу (3.7) обчислюємо річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки:

$$С = 0,21 \text{ x } 13400 + 909,28 + 0,46 \text{ x } 13400 = 9887,28 \text{ грн}$$

де $С_в$ – витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки (20% від капітальних витрат);

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки (46% від капітальних витрат);

$С_к$ – керування системою інформаційної безпеки.

Тепер розглянемо можливі втрати через припинення роботи корпоративного вузла чи через виток інформації.

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ви} = \sum З_о / F \text{ x } t_в = 101 \text{ x } 10 = 1010 \text{ грн}$$

Де середньогодинна заробітня плата обслуговуючого персоналу — 101 грн, а час відновлення після атаки $t_в = 10$ годин.

3.5 Визначення загального ефекта від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R – C, \qquad (3.10)$$

Де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн (врахуємо 2080 годин на рік);

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки (як вже підрахували 9887,28 грн).

Підрахуємо загальний ефект від впровадження системи інформаційної безпеки:

$$E = (101 \text{ x } 2080) \text{ x } 0{,}3 – 9887{,}28 = 53137 \text{ грн.}$$

Розрахуємо також оцінку економічної ефективності системи захисту інформації. Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = E / K , \quad (3.11)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, (приблизно 80000 тис. грн)

Підрахуємо коефіцієнт ROSI:

$$ROSI = 53137 / 80000 = 0,66$$

Можемо зробити висновок, що коефіцієнт повернення інвестицій вказує на перспективність інфвестицій.

Висновки до третього розділу

У дипломному проекту було визначено такі показники:

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають: К = 13400 грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки та становить: Е = 53137 грн, коефіцієнт ROSI становить 0,66

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають: С = 9887,28 грн

ВИСНОВКИ

У першому розділі проведено дослідження принципів хмарного обчислення даних та виділено три основні моделі обслуговування. Був проведений аналіз поточної ситуації в Україні та світі в галузі безпеки персональних даних. Проаналізовано приклади найбільших випадків кіберзлочинів за останній період.

Обґрунтовано актуальність проблеми захисту персональних даних у світовому масштабі при аналізі розвитку нормативної бази Європейського союзу з огляду на історичні події локального та глобального масштабів.

Було проведено аналіз основних вимог загального регламенту захисту даних, визначено його особливості.

Розглянуто нормативно-правову базу у сфері захисту інформації. Виділені основні закони, нормативні документи та державні стандарти, що стосуються розробки політики безпеки інформації на підприємстві.

У другому розділі було визначено основні етапи впровадження вимог загального регламенту захисту даних на прикладі однієї з трьох основних моделей обчислення хмарних технологій — SaaS. Визначено особливості цього методу.

Було розглянуто три способи збереження даних з різними видами шифрування. Відповідно до них було проведено аналіз інформаційних ризиків та визначено оптимальній спосіб збереження даних.

Розроблено рекомендації щодо впровадження загального регламенту захисту даних, дотримуючись результатів попередніх досліджень.

В економічній частині проведений розрахунок капітальних та експлуатаційних витрат на розробку і впровадження рекомендації по застосуванню GDPR.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про інформацію [Електронний ресурс] : закон України від 02.10.1992 № 2657-XII. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12.
2. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : закон України від 05.07.1994 № 80/94-ВР. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-вр.
3. Про електронні документи та електронний документообіг [Електронний ресурс] : закон України від 22.05.2003 № 851-IV. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/8515.
4. Про захист персональних даних . [Електронний ресурс] : закон України від 01.06.2010 № 2297-VI. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-51.
5. Постанова Кабінету міністрів України №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006
6. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»
7. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»,
8. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»
9. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»
10. Microsoft, керівництво по GDPR для бізнесу [Електронний ресурс]. – Режим доступу : https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/gdpr-compliance?view=o365-worldwide
11. IBM, підготовка до вступу GDPR [Електронний ресурс]. – Режим доступу : https://www.ibm.com/analytics/ru/ru/technology/general-data-protection-regulation/

12. Adobe, Стандарт кампании - Загальний стан речей про захист даних [Електронний ресурс]. – Режим доступу

13. Facebook, зобов'язання і підготовка до дотримання регламенту [Електронний ресурс]. – Режим доступу: https://www.facebook.com/business/gdpr

14. European Commission, Правила захисту персональних даних всередині і за межами ЄС [Електронний ресурс]. – Режим доступу https://ec.europa.eu/info/law/law-topic/data-protection_en.

15. Випадки витоку конфіденційної інформації в українських компаніях [Електронний ресурс]. – Режим доступу: https//:searchinform.com.ua/

16. Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh, and John C. Mitchell, "Client-side defence against web-based identity theft," in NDSS. The Internet Society, 2004.

17. GARTNER. "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks", December 17,2007, available: "http://www.gartner.com/it/page.jsp?id=565125"

18. Zhao, M., An, B. and Kiekintveld, C., 2016, February. Optimizing personalized email filtering thresholds to mitigate sequential spear phishing attacks. In Proceedings of the 30th AAAI Conference on Artificial Intelligence (AAAI).

19. G. Tally, R. Thomas, T. V. Vleck, "Anti-Phishing : Best Practices for Institutions and Consumers" Mcafee research technical report, September 2004.

20. Arachchilage, N. A. G. (2015). User-Centred Security Education: A Game Design to Thwart Phishing Attacks. arXiv preprint arXiv:1511.03459.

21. Srivastava; B. B. Gupta; A. Tyagi; A. Shamn; A. Mishra, "Recent Survey on DDoS Attacks and Defence Mechanisms," Advances in Parallel Distributed Computing, Communications in Computer and Information Science, vol. 203, pp. 570-580.

22. Wu, M., Miller, R. and Garfinkel, S., 2005. Do Security Toolbars Actually Prevent Phishing Attacks?, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montreal, Quebec, Canada, 22 - 27April 2006.

23. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol.29, no.7, pp. 1645–1660, 2013.

24. FireEye, “Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign”, Available at: https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

25. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия: учеб. пособие. – СПб.: БХВ-Петербург, 2003.- 752с.

26. Методичні рекомендації до підготовки та захисту дипломної роботи (проекту) для студентів галузі знань 1701 «Інформаційна безпека» та спеціальності 125 «Кібербезпека» / Т.В. Бабенко, М.В. Корнєєв, О.В. Кручінін, Д.С. Тимофєєв ; Нац. гірн. ун-т. – Д. : НГУ, 2016. – 44 с.

27. Методичні вказівки до виконання економічної частини дипломного проекту (для студентів напряму підготовки 1701 Інформаційна безпека)/ Упорядн.: О.Г. Вагонова, І.В. Шереметьєва, Ю.О. Волотковська, Н.М. Романюк. – Дніпропетровськ: ДВНЗ "Національний гірничий університет", 2013. – 17 с.

28. Amazon, Центр Загальних норм захисту даних (GDPR) [Електронний ресурс]. –https://www.w3schools.com/html/html_css.asp

29. FireEye, “Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign”, Available at: https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

30. ROWAN UNIVERSITY, Стандарт, який регулює захист даних і конфіденційність для фізичних осіб в межах Європейського Союзу [Електронний ресурс]. – Режим доступу : https://confluence.rowan.edu/display/POLICY/GDPR+-+Standard+Governing+Data+Protection+and+Privacy

31. Chorley, Стандарт конфиденциальности GDPR [Електронний ресурс]. – Режим доступу :http://chorley.gov.uk/Documents/GDPR/Data%20Protection%20Policy.pdf

32. OU, Що варто знати про GDPR [Електронний ресурс]. – Режим доступу https://dou.ua/lenta/articles/what-gdpr-is/

33. CITRIX, Загальний стан речей про захист даних (GDPR) [Електронний ресурс]. – Режим доступу:https://www.citrix.com/it-security/gdpr-faq.html

34. Smartsolutions, Обробка персональних даних за європейськими правилами[Електронний ресурс]. – Режим доступу

35. Intersoft Consulting, Загальне правило захисту даних GDPR[Електронний ресурс]. – Режим доступу:https://gdpr-info.eu/

36. Закон про захист персональних даних [Електронний ресурс]. – Режим доступу :http://zakon.rada.gov.ua/laws/show/2297-17

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат		
2	А4	Зміст		
3	А4	Вступ		
4	А4	1 Розділ		
5	А4	2 Розділ		
6	А4	3 Розділ		
7	А4	Висновки		
8	А4	Перелік посилань		
9	А4	Додаток А		
10	А4	Додаток Б		
11	А4	Додаток В		
12	А4	Додаток Г		

ДОДАТОК Б. Відгук керівника економічного розділу

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Керівник : _____ к.е.н.,доц. Пілова Д.П.

(підпис)

ДОДАТОК В. Відгук керівника дипломної роботи

ВІДГУК

на дипломну роботу магістра

студентки групи 125м-17-2

Шушпанової Анастасії Русланівни

на тему: «Особливості впровадження загального регламенту захисту даних (GDPR) в хмарних технологіях»

Метою дипломної роботи є вдосконалення сучасних методів протидії кібершахрайству, надання і впровадження рекомендацій.

Тема дипломного проекту безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в дипломному проекті вирішуються наступні задачі: визначення особливостей впровадження регламенту при використанні хмарних технологій; формування етапів підготовки до впровадження вимог GDPR у SaaS-моделі; проведення аналізу інформаційних ризиків; розробка шаблонів для впровадження GDPR у сфері хмарних технологій. .

Розроблено рекомендації щодо впровадження загального регламенту захисту даних, дотримуючись попередніх досліджень. Практичне значення результатів дипломного проекту полягає у розробці рекомендацій щодо впровадження загального регламенту захисту даних для власників інформації.

Оформлення пояснювальної записки до дипломної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Шушпанова А.Р. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння звання магістра та кваліфікації професіонала з організації інформаційної безпеки.

Дипломна робота заслуговує оцінки «відмінно».

Керівник дипломної роботи д.ф.-м.н., проф. Кагадій Т.С.

Керівник спец. розділу ст. викл. Тимофєєв Д.С.

ДОДАТОК Г. Перелік файлів на електронному носії

1. Дипломний проект Шушпанова А.Р. 125М-17-2 – Пояснювальна записка.
2. Шушпанова А.Р. 125М-17-2.pttx – Презентація.