МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет прикладної математики та інформатики
(повне найменування назва факультету)

кібербезпеки
(повна назва кафедри)

Дипломна робота

Розробка проекту проведення аудиту веб-ресурсів на відповідність вимогам GDPR

Виконав: студент групи ПМК-42с
спеціальності
125 «Кібербезпеки»
(шифр і назва спеціальності)

(підпис) Федоренко І.
(прізвище та ініціали)

Керівник (підпис) Вайганг Г.О.
(прізвище та ініціали)

Рецензент (підпис) О.Є. Ігарюнов
(прізвище та ініціали)

2023

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ФРАНКА

Факультет Прикладної математики та інформатики
Кафедра Кібербезпеки
Спеціальність: 125 «Кібербезпека»
«шифр і назва»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри _____

"31 "серпня 2022 року

ЗАВДАННЯ
на кваліфікаційну бакалаврську роботу студента
Федоренко Ірини
(прізвище, ім'я, по батькові)

1. **Тема роботи**: Розробка проекту проведення аудиту веб-ресурсів на відповідність вимогам GDPR
   Керівник роботи доцент, к.т.н. Вайганг Г.О.
   затверджені наказом університету від «13» вересня 2021 року № 15
2. **Строк подання студентом роботи** «13» червня 2023 року
3. **Вихідні дані до роботи:** _____

4. **Зміст пояснювальної записки (перелік питань, які потрібно розробити)**
1. Поняття персональних даних та їх обробка відповідно чинного законодавства
2.. Характеристика «Загальний регламент захисту даних (GDPR)
3. Аудит інформаційної безпеки як інстумент захисту персональних даних
4. Основні етапи підготовки до впровадження аудиту за принципами GDPR
5. Аутентифікація у веб-ресурсах як елемент захисту персональних даних

5. **Перелік графічного матеріалу:**

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання **31 серпня 2022 р.**

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Уточнення постановки завдання	21.03.2023	
2	Аналіз літератури	28.03.2023	
3	Обґрунтування вибору рішення	31.03.2023	
4	Збір даних	07.04.2023	
5	Поняття персональних даних, їх обробка	18.04.2023	
6	Характеристика GDPR. Аудит інф. системи	28.04.2023	
7	Впроваджена аудиту. Автентифікація у веб	12.05.2023	
8	Оформлення та друк пояснювальної записки	25.05.2023	
9	Оформлення презентації	06.06.2023	
10	Отримання рецензії	10.06.2023	
11	Подання роботи на кафедру	12.06.2023	
12	Захист в ЕК	16.06.2023	

Студент _____ Федоренко І.
(підпис) (ініціали, прізвище)

Керівник роботи _____ ВайгангГ.О.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Пояснювальна записка дипломного проекту складається зі вступу, п’яти розділів, що містять 22 рисунки, висновків та списку використаних джерел з 40 найменувань. Загальний обсяг роботи становить 88 сторінки.

Об’єктом дослідження є безпека персональних даних.

Предметом дослідження є методи захисту персональних даних веб-ресурсів та методики перевірки відповідності до вимог GDPR.

Мета роботи полягає в розробці інструментів захисту персональних даних з метою перевірки їх відповідності вимогам, встановленим Загальним регламентом про захист персональних даних (GDPR).

У першому розділі розглядається поняття персональних даних, їх важливість та актуальність у сучасному світі. Проводиться аналіз нормативно-правових актів, які регулюють захист персональних даних, та обговорюються питання обробки персональних даних.

У другому розділі проводиться огляд тенденцій щодо захисту персональних даних і представляється базова інформація про Загальний регламент захисту даних (GDPR). Розглядаються базові принципи GDPR та технічні заходи, що сприяють захисту персональних даних. Також детально аналізуються вимоги GDPR щодо захисту персональних даних.

У третьому розділі проводиться аналіз загроз безпеці персональної інформації та веб-ресурсів. Розглядаються основні питання аудиту інформаційної безпеки та представляються види аудиту веб-ресурсів та інструменти їх проведення. Висвітлюються важливі аспекти аудиту, спрямованого на захист персональних даних.

У четвертому розділі розглядаються основні етапи підготовки до впровадження аудиту з відповідності вимогам GDPR. Подається алгоритм процесу встановлення відповідності до вимог GDPR, визначаються заходи на відповідність Загальному регламенту по захисту даних. Розглядається формування моделей порушника та загроз під регулюванням GDPR та визначаються цілі проекту аудиту веб-ресурсів на відповідність вимогам GDPR.

У п’ятому розділі обґрунтовується важливість аутентифікації як елемента захисту персональних даних у веб-ресурсах. Розглядаються підходи і методи аутентифікації, а також існуючі системи аутентифікації/авторизації та обрані механізми для їх реалізації. Описується структура модуля та реалізовані алгоритми автентифікації. Представляється середовище розробки та програмна реалізація аутентифікаційного модуля та проводиться опис структури програми та тестування.

Ключові слова: ПЕРСОНАЛЬНІ ДАНІ, ВЕБ-РЕСУРС, GDPR, ЄВРОПЕЙСЬКИЙ СОЮЗ, БЕЗПЕКА ДАНИХ, ЗАГРОЗИ, АУДИТ, АВТЕНТИФІКАЦІЯ.

ABSTRACT

The explanatory note of the diploma project consists of an introduction, five chapters containing 22 figures, conclusions and a list of 40 references. The total volume of the work is 88 pages.

The **object** of research is personal data security.

The **purpose** of the work is to develop tools for protecting personal data in order to verify their compliance with the requirements established by the General Data Protection Regulation (GDPR).

The first section discusses the concept of personal data, its importance and relevance in the modern world. It analyzes the legal acts regulating the protection of personal data and discusses the issues of personal data processing.

The second section reviews trends in personal data protection and provides basic information on the General Data Protection Regulation (GDPR). The basic principles of the GDPR and technical measures that contribute to the protection of personal data are discussed. The GDPR requirements for personal data protection are also analyzed in detail.

The third section analyzes threats to the security of personal information and web resources. The main issues of information security audit are considered and the types of web resource audits and tools for their implementation are presented. Important aspects of an audit aimed at protecting personal data are highlighted.

The fourth section discusses the main stages of preparation for the implementation of a GDPR compliance audit. It presents an algorithm for the process of establishing compliance with the GDPR requirements, identifies measures for compliance with the General Data Protection Regulation. The article discusses the formation of offender and threat models under the GDPR and defines the objectives of the project of auditing web resources for compliance with the GDPR.

The fifth section substantiates the importance of authentication as an element of personal data protection in web resources. The approaches and methods of authentication are considered, as well as existing authentication/authorization systems and selected mechanisms for their implementation. The module structure and implemented authentication algorithms are described. The development environment and software implementation of the authentication module are presented, and the program structure and testing are described.

Keywords: PERSONAL DATA, WEB RESOURCE, GDPR, EUROPEAN UNION, DATA SECURITY, THREATS, AUDIT, AUTHENTICATION.

Зміст

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

EDPB	–	European Data Protection Board (Європейська Рада Захисту Даних)
GDPR	–	General Data Protection Regulation (Загальний регламент про захист даних)
ЄС	–	Європейський Союз
ІБ	–	інформаційна безпека
ПД	–	персональні дані
КВ	–	коефіцієнт вагомості
ІСПД	–	Інформаційні системи персональних даних
	–	

ВСТУП

Актуальність. Серед основних принципів політики «цифровізації України» відзначається положення про те, що цей процес «має супроводжуватися підвищенням довіри і безпеки при використанні інформаційно-комп'ютерних технологій».

Тобто фактично аргументується необхідність вживання заходів, спрямованих на зміцнення довіри користувачів Інтернет до джерел інформації, включаючи інформаційну безпеку, кібербезпеку, захист конфіденційності персональної інформації.

Так як, персональні дані є однією з найбільш конвертованих валют у сучасному світі , то потреба їх захисту не є примхою людини, яка не бажає розголошувати забагато інформації про себе в цифровому середовищі, – персональні дані користувачів (клієнтів) стають головним джерелом конкурентоспроможності суб'єкта господарювання.

Як відомо, захист персональних даних – проблема, яка вже достатньо давно є актуальною не лише для великих компаній, державних підприємств або веб-ресурсів. Але зараз прийшов час, коли це питання повинно стати справжнім викликом для українських сайтів, які в своїй діяльності використовують персональні дані громадян та жителів Європейського Союзу.

Відомо, що 25 травня 2018 року в юридичному полі Європейського Союзу вступив в силу новий нормативний акт - Загальний Регламент Захисту Даних, більш відомий як GDPR (General Data Protection Regulation), що посилює захист персональної інформації. Європейський союз переходить на нові правила поводження з персональними даними, а Регламент стосується будь-якої роботи компаній з персональними даними клієнтів, а саме: збору, зберігання, передачі.

Тема є неймовірно актуальною, адже українські веб-ресурси та підприємці все більше виходять на європейський ринок і сама країна стає ближче до Європи. Це висуває необхідність відповідати загальноприйнятим нормам і вміти пристосовуватися до них. В той же час, методики із встановлення відповідності

GDPR продовжують розроблятись та вдосконалюватись, і у відкритому доступі практично відсутні.

Мета роботи полягає в розробці інструментів захисту персональних даних з метою перевірки їх відповідності вимогам, встановленим Загальним регламентом про захист персональних даних (GDPR).

Відповідно до поставленої мети були сформовані наступні завдання:

1. дослідити основні питання, щодо поняття персональних даних на веб-ресурсах та визначити існуючи загрози;
2. провести аналіз загроз безпеки веб-ресурсів, вразливостей та механізмів захисту;
3. дослідити нормативно-правової бази щодо захисту персональних даних та аналіз вимог GDPR;
4. розробити методику аудиту, включаючи набір критеріїв, шаблони аудиту та план проведення, з урахуванням особливостей веб-ресурсів і вимог GDPR.;
5. визначити базові критерії та вимоги відповідності GDPR;
6. розробка інструмент захисту персональних даних відповідно до норм GDPR та перевірити існуючого стану захисту даних користувачів до правил GDPR.

Об’єктом дослідження є безпека персональних даних.

Предметом дослідження є методи захисту персональних даних веб-ресурсів та методики перевірки відповідності до вимог GDPR.

РОЗДІЛ 1.
ПОНЯТТЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЇХ ОБРОБКА ВІДПОВІДНО ЧИННОГО ЗАКОНОДАВСТВА

1.1 Поняття персональних даних та актуальність їх захисту

Глобалізація разом із швидким технологічним розвитком, особливо зараз, коли цифровізація є рушійною силою в усіх галузях промисловості, поставили нові виклики щодо захисту персональних даних. Фактом є те, що кіберінциденти продовжують висхідну траєкторію до другого за важливістю бізнес-ризику (40%) , тоді як п’ять років тому він займав 15 місце.

Завдяки глобалізації та швидкому обміну інформацією сталося значне збільшення обсягу персональних даних, які збираються, обробляються та передаються. Це створює потребу у засадничих змінах в захисті цих даних, оскільки вони можуть перетинати кордони країн і потрапляти в різні юрисдикції.

З розвитком технологій зростають також кіберзагрози. Хакери та зловмисники активно шукають способи проникнення до систем та крадіжки персональних даних. Глобальний характер цифрового світу означає, що захист персональних даних стає завданням масштабним і складним [1].

Так звані «кіберурагани», коли хакери порушують роботу великої кількості компаній через загальну залежність від інфраструктури Інтернету, зростають. З одного боку, технологічні інновації пропонують нові способи пом’якшення ризику, але з іншого – створюють нові небезпеки.

Очікується, що автономні машини, штучний інтелект (ШІ), оцифровані ланцюги поставок і краще використання даних і аналітики запропонують широкий спектр можливостей і забезпечать більшу продуктивність і більш індивідуальні пропозиції для клієнтів, тоді як автоматизація розглядається як засіб підвищення безпеки для мінімізації людського впливу. помилка. Однак останні дослідження свідчать про те, що вразливість підключених систем до системних збоїв або злому та інших зловмисних кіберакцій, таких як здирництво та шпигунство, у майбутньому зростатиме [1].

Сучасні суспільні відносини характеризується широким використанням персональних даних під час обігу інформації (соціального, фінансового, правоохоронного, науково-технічного та ін. характеру), що вимагає не тільки вільний рух інформації про особу, але й забезпечення її надійного захисту у відповідності до основних прав і свобод людини [2].

Визначення поняття персональні дані наводиться в абзаці восьмому статті 2 Закону, відповідно до якого персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Але законодавством України не встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, задля можливості застосування положень Закону до різноманітних ситуацій, в тому числі при обробці персональних даних в інформаційних (автоматизованих) базах та картотеках персональних даних, що можуть виникнути у майбутньому, у зв’язку зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя.

Персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [3].

Відповідно до Закону, обробка персональних даних – це «будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем» .

Всупереч поширеному помилковому твердженню обробкою є не лише вчинення вказаних дій із систематизованою сукупністю персональних даних великої кількості осіб (базою даних, реєстром, каталогом, досьє тощо). Просте зберігання володільцем, навіть у недоступному вигляді, інформації про хоча б одного суб’єкта персональних даних є обробкою відповідно до положень Закону. Таким чином, наявність будь-якого документу, що містить персональні дані особи, на робочому столі чи в сейфі державного службовця становитиме обробку персональних даних цієї особи.

Рисунок 1.3 – Перелік заходів щодо забезпечення безпеки ПД під час їхньої обробки

Цей список не є вичерпним, тобто законом допускаються інші дії, спрямовані на безпеку персональних даних.

Висновки до розділу 1

У даному розділі було розглянуто питання визначення поняття «персональні дані» та їх характеристики. Персональні дані включають будь-яку інформацію, яка стосується ідентифікованої або ідентифікованої фізичної особи. Це можуть бути імена, адреси, номери телефонів, електронні адреси, фотографії та інші дані, які дозволяють прямо або опосередковано ідентифікувати особу.

Обробка персональних даних включає будь-яку операцію або набір операцій, які здійснюються з персональними даними, такі як збір, збереження, організація, структурування, зміна, використання, передача та видалення.

Існує значна кількість законів та регуляторних актів, які регулюють обробку персональних даних, зокрема Загальний регламент про захист даних

(GDPR) в Європейському Союзі. Ці закони встановлюють права суб'єктів даних та обов'язки для організацій, що обробляють персональні дані.

Вимоги до обробки персональних даних базуються на таких принципах, як законність, справедливість та прозорість, обмеження цілей, мінімізація даних, точність, обмеження зберігання, цілісність та конфіденційність, а також відповідність.

Згода суб'єкта даних є важливим елементом в обробці персональних даних. Згода повинна бути недвозначною, вільною, інформованою та конкретною. Суб'єкти даних мають право відкликати свою згоду в будь-який час.

Організації, які обробляють персональні дані, мають обов'язок дотримуватися законодавчих вимог щодо захисту цих даних. Вони повинні забезпечити відповідну безпеку даних, здійснювати відповідність з законом, надавати інформацію суб'єктам даних та виконувати їх права.

За порушення законодавства про персональні дані можуть бути передбачені серйозні штрафи та інші санкції. Організації повинні бути свідомі ризиків та вживати необхідні заходи для дотримання вимог законодавства.

Усі ці аспекти важливі для забезпечення захисту персональних даних та дотримання вимог чинного законодавства. При обробці персональних даних, організації повинні дотримуватися принципів та встановлених процедур, а також забезпечити відповідність вимогам законодавства, щоб забезпечити приватність та конфіденційність персональних даних суб'єктів даних.

РОЗДІЛ 2.
ХАРАКТЕРИСТИКА «ЗАГАЛЬНИЙ РЕГЛАМЕНТ ЗАХИСТУ ДАНИХ (GDPR)

2.1 Огляд тенденцій щодо захисту персональних даних

Захист персональних даних отримав значний акцент у регуляторній сфері. Країни впроваджують законодавство та регуляторні вимоги щодо захисту персональних даних, такі як GDPR в Європейському Союзі. Організації, що мають глобальний присутній та операції, повинні відповідати різноманітним нормам та вимогам у сфері захисту даних.

Щоб усунути такі ризики та встановити принципи прозорого використання персональних даних, ЄС прийняв 27.04.2016 р. Загальний регламент захисту даних (GDPR) № 2016/679, який безпосередньо застосовується до всіх держав-членів ЄС. Регламент вимагає від усіх організацій, що надають послуги або обробляють дані, пов’язані з громадянами ЄС, дотримуватися його, навіть якщо організації розташовані за межами ЄС. Спосіб, яким бізнес керує витоком даних, безпосередньо впливає на кінцеву вартість.

Відповідно до Загальний регламент захисту даних (The General Data Protection Regulation - GDPR), можна зазначити, що «регламент передбачає захист фізичних осіб щодо обробки персональних даних, що є фундаментальним правом (стаття 8 (1) Хартії основних прав Європейського Союзу (ЄС) та стаття 16 (1) Договору про функціонування Європейського Союзу (TFEU) Відповідно до документу принципи та правила захисту фізичних осіб при поводженні з їх особистими даними повинні незалежно від їх національності чи місця проживання, поважати їх основні права і свободи, зокрема їхнє право на захист персональних даних. Регламент застосовується при обробці персональних даних установами, органами, організаціями та агентствами Євросоюзу».

Персональні дані відповідно до Регламенту поділяються на категорії:

- генетичні дані (genetic data),
- біометричні дані (biometric data),

Таким чином, здійснюючи обробку ПД, потрібно вживати максимальних заходів щодо захисту даних і не надавати можливості стороннім особам користуватися такими даними. Разом з тим, необхідно встановлювати чіткий режим доступу до ПД, офіційно розподіляючи обов’язки щодо обробки даних між конкретними працівниками та іншими зацікавленими особами.

Висновки до розділу 2

Узагальнюючи проведені дослідження, можна зазначити, що загальний регламент захисту даних (GDPR) є важливим законодавчим актом, який регулює обробку та захист персональних даних в Європейському Союзі. Його ціль полягає в забезпеченні прав і свобод фізичних осіб та захисті їх приватності у зв'язку з обробкою їх персональних даних.

GDPR встановлює широкий спектр прав суб'єктів даних, зокрема право на доступ до їх персональних даних, право на виправлення, право на видалення, право на обмеження обробки, право на перенесення даних та право на виключення від автоматизованого прийняття рішень.

GDPR вимагає від організацій, що обробляють персональні дані, встановлення внутрішніх політик та процедур забезпечення відповідності вимогам регламенту. Це включає укладання угод про обробку даних з підрядниками, проведення оцінки впливу на захист даних та вживання заходів забезпечення безпеки даних.

GDPR передбачає обов'язок повідомлення про порушення безпеки даних, що може стати загрозою для прав і свобод суб'єктів даних, до відповідних регуляторних органів та суб'єктів даних. Це сприяє забезпеченню прозорості та вчасного реагування на подібні порушення.

GDPR встановлює великі штрафи за порушення вимог регламенту, які можуть сягати до 4% глобального річного обороту організації або 20 млн євро, в залежності від того, яка сума буде більшою. Це надає стимул організаціям серйозно ставитися до захисту персональних даних і дотримуватися вимог GDPR.

GDPR має екстериторний характер, тобто його вимоги застосовуються до організацій не тільки в Європейському Союзі, але й до організацій з-за меж ЄС, які обробляють дані європейських суб'єктів даних. Це робить GDPR важливим для глобальних бізнесів та організацій, які мають зв'язок з ЄС.

Усі ці аспекти підкреслюють важливість відповідності вимогам GDPR для організацій, які обробляють персональні дані, і необхідність впровадження ефективних політик та процедур забезпечення відповідності цим вимогам.

РОЗДІЛ 3.
АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ІНСТУМЕНТ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. Аназіз загроз безпеки персональній інформації та веб-ресурсам

Загрози безпеки — це певна сукупність умов або факторів, що впливають, які створюють небезпеку щодо персональних даних, що полягає в ознайомленні сторонніх осіб з персональними даними, що захищаються, несанкціонованій зміні, знищенні, поширенні, а також інших неправомірних дій з персональними даними.

Джерелами загроз безпеці персональних даних можуть бути як внутрішні порушники, тобто власні співробітники, так і зовнішні порушники, які використовують як реалізацію загрози канали зв'язку, комп'ютерні мережі та Інтернет. Крім того, загрози безпеці можуть виникати при впровадженні в інформаційну систему шкідливих програм та вірусів.

Способами реалізації загроз безпеки може бути несанкціонований доступом до інформації, витік технічних каналів, і навіть спеціальні на персональні дані чи інформаційну систему.

Загрози несанкціонованого доступу до персональних даних, що обробляються в інформаційній системі, можуть здійснюватися за допомогою програмних та апаратно-програмних засобів. При цьому відбувається порушення режиму конфіденційності щодо персональних даних шляхом їхнього неправомірного копіювання та/або поширення. Також персональні дані, що захищаються, можуть бути змінені або знищені порушником, що може також спричинити значні наслідки.

У ході реалізації загрози несанкціонованого доступу можуть бути створені позаштатні режими роботи операційного середовища або програмного забезпечення, які можуть бути використані порушником для крадіжки інформації або впливу на неї ззовні.

конфіденційність та інші відповідні документи, які регулюють обробку персональних даних на веб-ресурсі.

Цілі аудиту допомагають забезпечити відповідність веб-ресурсу вимогам GDPR та захист персональних даних користувачів.

Висновки по розділу 4

В цьому розділі були описані практичні кроки відповідності до вимог GDPR, зображені діаграми потоку даних, виділені основні компоненти типового веб-ресурсу, на основі яких було складено моделі загроз та порушника.

Детально описано правила складання основних документів з прикладами, зокрема політика конфіденційності, cookies, політику оплати умови використання. Зазначено вимоги для сторінки реєстрації та особистого профіля.

Окремо було сказано про технічні заходи, яких вимагає GDPR, а саме те, що архітектура системи має будуватися за принципом Data protection by design and by default.

РОЗДІЛ 5.
АУТЕНТИФІКАЦІЯ У ВЕБ-РЕСУРСАХ ЯК ЕЛЕМЕНТ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

5.1. Обґрунтування підходів і методів аутентифікації

Веб-ресурси використовують клієнт-серверні технології, що передбачають взаємодію між користувачем (клієнтом) і сервером, на якому розміщений веб-сайт чи додаток. Ця взаємодія може бути розбита на три основних етапи: автентифікація, обмін даними та вихід із системи.

Перший етап – автентифікація. Цей етап включає процес перевірки ідентифікації користувача, тобто встановлення, що користувач є дійсною особою, яка має право доступу до системи. Це може включати введення логіну та пароля, використання біометричних даних (таких як відбиток пальця або розпізнавання обличчя) або інші методи аутентифікації. При коректності даних система аутентифікації та авторизації генерує ідентифікатор сесії і відправляє його на сторону клієнта, як показано на рис. 5.1.

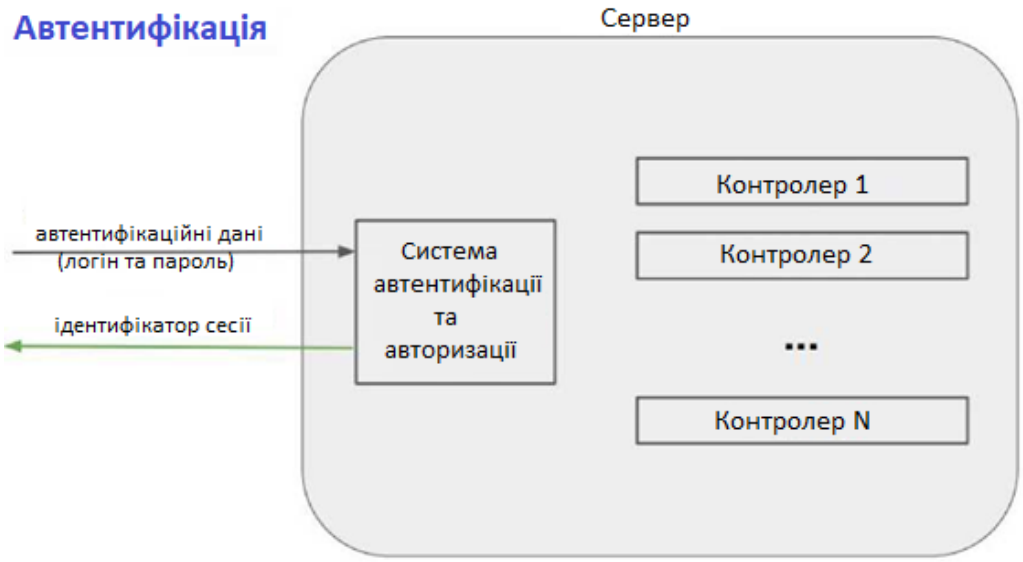

Рисунок 5.1 – Автентифікація з допустимими даними автентифікації

Якщо дані аутентифікації невірні, система аутентифікації та авторизації повертає на сторону клієнта відповідь на помилку, як показано на рис. 5.2.

2. LoginRouteHandler - функція, що реалізує роботу блоку обробки вхідних запитів для етапу аутентифікації.
3. SecureRouteHandler - функція, яка реалізує роботу блоку обробки вхідних запитів на етапі обміну даними з системою, і перевіряє ідентифікатор сесії.
4. LogoutRouteHandler - функція, що реалізує роботу блоку обробки вхідних запитів на вихід з системи.

Кожна з функцій має 4 параметри:

- request - об'єкт запиту, відправлений від клієнта.
- response - об'єкт відповіді на запит.
- next - функція виклику наступного обробника.
- config - конфігураційний файл модуля "SecureAuthenticationModule".

Інструкція до файлу конфігурації наведено в Додатку Б.

Для наочного прикладу практичного використання модуля "SecureAuthenticationModule" зберігання даних про суб'єктів та їх сеанси проілюстровано на серверних змінних (Додаток А).

Для тестування модуля був розроблений прототип клієнт-серверного веб-додатку та протестовані наступні реалізовані механізми:

1. Механізм реалізації розсилки SMS-повідомлень.
2. Механізм реалізації одноразової перевірки пароля за допомогою програми Google Authenticator.

Використання модуля з різними параметрами конфігураційного файлу.

А також були протестовані можливості модуля, а саме:

1. Можливість додати перевірку аутентифікації певних дій в системі.
2. Можливість налаштувати метод аутентифікації для всіх користувачів системи, причому для кожного індивідуально.

В результаті тестування було прийнято рішення про впровадження модуля аутентифікації та авторизації «SecureAuthenticationModule» з багатофакторним контролем доступу в серверну частину веб-додатку.

Висновки до розділу 5

В даному розділі були розглянуті сучасні підходи до аутентифікації як інструменту захисту персональних даних. В процесі дослідження були обрані підходи і технології для реалізації різних механізмів аутентифікації, а також реалізовано модуль аутентифікації і авторизації з підтримкою багатофакторного контролю доступу дій в системі.

Крім того, була розроблена структура модуля "SecureAuthenticationModule" і оформлений конфігураційний файл з можливістю налаштування модуля для різних реалізацій веб-додатків, що забезпечує його масштабованість. В результаті модуль "SecureAuthenticationModule" був реалізований на платформі NodeJS, а також проаналізована його застосовність в реальному додатку.

ВИСНОВКИ

Узагальнюючи проведені дослідження, можна зазначити, що загальний регламент захисту даних (GDPR) є важливим законодавчим актом, який регулює обробку та захист персональних даних в Європейському Союзі. Його ціль полягає в забезпеченні прав і свобод фізичних осіб та захисті їх приватності у зв'язку з обробкою їх персональних даних.

Під час роботи над темою було розглянуто питання визначення поняття «персональні дані» та їх характеристики. Персональні дані включають будь-яку інформацію, яка стосується ідентифікованої або ідентифікованої фізичної особи. Це можуть бути імена, адреси, номери телефонів, електронні адреси, фотографії та інші дані, які дозволяють прямо або опосередковано ідентифікувати особу.

Обробка персональних даних включає будь-яку операцію або набір операцій, які здійснюються з персональними даними, такі як збір, збереження, організація, структурування, зміна, використання, передача та видалення.

Існує значна кількість законів та регуляторних актів, які регулюють обробку персональних даних, зокрема Загальний регламент про захист даних (GDPR) в Європейському Союзі. Ці закони встановлюють права суб'єктів даних та обов'язки для організацій, що обробляють персональні дані.

Вимоги до обробки персональних даних базуються на таких принципах, як законність, справедливість та прозорість, обмеження цілей, мінімізація даних, точність, обмеження зберігання, цілісність та конфіденційність, а також відповідність.

Згода суб'єкта даних є важливим елементом в обробці персональних даних. Згода повинна бути недвозначною, вільною, інформованою та конкретною. Суб'єкти даних мають право відкликати свою згоду в будь-який час.

Організації, які обробляють персональні дані, мають обов'язок дотримуватися законодавчих вимог щодо захисту цих даних. Вони повинні забезпечити відповідну безпеку даних, здійснювати відповідність з законом, надавати інформацію суб'єктам даних та виконувати їх права.

За порушення законодавства про персональні дані можуть бути передбачені серйозні штрафи та інші санкції. Організації повинні бути свідомі ризиків та вживати необхідні заходи для дотримання вимог законодавства.

Усі ці аспекти важливі для забезпечення захисту персональних даних та дотримання вимог чинного законодавства. При обробці персональних даних, організації повинні дотримуватися принципів та встановлених процедур, а також забезпечити відповідність вимогам законодавства, щоб забезпечити приватність та конфіденційність персональних даних суб'єктів даних.

GDPR встановлює широкий спектр прав суб'єктів даних, зокрема право на доступ до їх персональних даних, право на виправлення, право на видалення, право на обмеження обробки, право на перенесення даних та право на виключення від автоматизованого прийняття рішень.

Отже, аудит інформаційної безпеки є важливою складовою для забезпечення захисту персональних даних в організаціях та на веб-ресурсах. Він дозволяє оцінити ефективність і надійність заходів безпеки, ідентифікувати потенційні загрози та вразливості, а також розробити рекомендації щодо поліпшення захисту даних.

Аудит інформаційної безпеки повинен охоплювати всі аспекти обробки персональних даних, включаючи їх збір, зберігання, обробку, передачу та захист. Він вимагає перевірки дотримання внутрішніх політик та процедур, оцінки ефективності технічних та організаційних заходів безпеки, а також виявлення можливих ризиків і порушень.

Результати аудиту інформаційної безпеки слід використовувати для вдосконалення системи захисту персональних даних. Це може включати впровадження додаткових заходів безпеки, проведення навчання та свідомості персоналу щодо захисту даних, оновлення політик та процедур, а також вдосконалення технічних рішень.

В роботі були описані практичні кроки відповідності до вимог GDPR, зображені діаграми потоку даних, виділені основні компоненти типового веб-ресурсу, на основі яких було складено моделі загроз та порушника.

Детально описано правила складання основних документів з прикладами, зокрема політика конфіденційності, cookies, політику оплати умови використання. Зазначено вимоги для сторінки реєстрації та особистого профіля.

Окремо було сказано про технічні заходи, яких вимагає GDPR, а саме те, що архітектура системи має будуватися за принципом Data protection by design and by default.

В роботі розглянуто методики оцінювання відповідності типового веб-ресурсу вимогам Загального регламенту про захист даних. Було проведено аналіз вимог GDPR та особливостей їх застосування; зокрема:

- проаналізовано основні статті Регламенту;
- побудовані моделі загроз та порушника безпеки веб-ресурсу;
- проаналізовано вимоги , що стосуються технічних заходів, яких вимагає GDPR

В роботі були розглянуті сучасні підходи до аутентифікації як інструменту захисту персональних даних. В процесі дослідження були обрані підходи і технології для реалізації різних механізмів аутентифікації, а також реалізовано модуль аутентифікації і авторизації з підтримкою багатофакторного контролю доступу дій в системі.

Крім того, була розроблена структура модуля "SecureAuthenticationModule" і оформлений конфігураційний файл з можливістю налаштування модуля для різних реалізацій веб-додатків, що забезпечує його масштабованість. В результаті модуль "SecureAuthenticationModule" був реалізований на платформі NodeJS, а також проаналізована його застосовність в реальному додатку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Albrecht, Jan Philipp. How the GDPR will change the world. Eur. Data Prot. L. Rev., 2016, 2: 287.
2. Joseph, Mathew M.; Framenau, Volker W. Systematic review of a new orb-weaving spider genus (Araneae: Araneidae), with special reference to the Australasian-Pacific and South-East Asian fauna. Zoological Journal of the Linnean Society, 2012, 166.2: 279-341.
3. LI, He; YU, Lu; HE, Wu. The impact of GDPR on global technology development. Journal of Global Information Technology Management, 2019, 22.1: 1-6.
4. Sirur, Sean; Nurse, Jason RC; Webb, Helena. Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In: Proceedings of the 2nd International Workshop on Multimedia Privacy and Security. 2018. p. 88-95.
5. Shabani, Mahsa; BORRY, Pascal. Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. European Journal of Human Genetics, 2018, 26.2: 149-156.
6. Dadkhah, Mehdi; BECK, Michael; JAZI, Mohammad. Cross Site Scripting Vulnerability in Web Application: Review and Preventive Approach. Journal of Applied Sciences Research, 2014, 10.8: 53-57.
7. Prokhorenko, Victor; CHOO, Kim-Kwang Raymond; ASHMAN, Helen. Web application protection techniques: A taxonomy. Journal of Network and Computer Applications, 2016, 60: 95-112.
8. Скембрей, Дж., Шема, М. Секреты хакеров. Безопасность Web-приложений - готовые решения. Скембре, Дж., Шема М – М.: Издательский дом «Вильямс» , 2013. — 384 с.
9. OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks, 2017. - (creative commons)

30. ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2008, IDT).
31. 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.
32. IBM, підготовка до вступу GDPR [Електронний ресурс]. - Режим доступу: https://www.ibm.com/analytics/ru/ru/technology/general-data-protection-regulation/
33. Auzy [Електронний ресурс] - Режим доступу: https://github. com/alexey-detr/auzy.
34. ExpressJS. NodeJS Web Application Framework [Електронний ресурс] - Режим доступу: https://expressjs. com/ru/
35. ExpressJS middleware. Використання проміжних обробників [Електронний ресурс] - Режим доступу: https://expressjs. com/ru/guide/using-middleware. HTML.
36. Google Authenticator [Електронний ресурс] - Режим доступу: https://te-st. en/entries/google-authenticator/
37. Multi-factor authentication [Електронний ресурс] - Режим доступу: https://www. Onelogin. com/learn/what-is-mfa .
38. NodeJS [Електронний ресурс] - Режим доступу: https://nodejs. org/uk/
39. RFC 6238. TOTP: Time-Based One-Time Password Algorithm. - Режим доступу: https://tools.IETF.org/html/rfc6238.
40. RFC 6265. HTTP State Management Mechanism [Електронний ресурс] - Режим доступу: https://tools. IETF. org/html/rfc6265.