НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«До захисту допущено»

В.о. завідувача кафедри

_____М.В.Грайворонський
(підпис)

“_____”_____2019р.

Дипломна робота
на здобуття ступеня бакалавра

з напряму підготовки6.170101 «Безпека інформаційних і комунікаційних систем»

на тему: Методика оцінки відповідності веб-ресурсу вимогам GDPR

_____

_____

Виконав (-ла): студент (-ка) 4 курсу, групи ФБ-51
(шифр групи)

Бурдело Євгеній Вікторович (підпис)
(прізвище, ім’я, по батькові)

Керівник доцент кафедри ІБ, к.т.н.,Стьопочкіна І.В. (підпис)
(посада, науковий ступінь, вчене звання, прізвище та ініціали)

Консультант _____ _____ _____ (підпис)
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали)

Рецензент _____ (підпис)
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ - 2019 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Напрям підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

_____ М.В.Грайворонський
(підпис)

«___»_____2019 р.

ЗАВДАННЯ
на дипломну роботу студенту

Бурдело Євгеній Вікторович
(прізвище, ім'я, по батькові)

1. Тема роботи: Методика оцінки відповідності веб-ресурсу вимогам GDPR, науковий керівник роботи: Стьопочкіна Ірина Валеріївна, к.т.н.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «27» травня 2019 р. № 1414-с

2. Термін подання студентом роботи 10 червня 2019 р.

3. Вихідні дані до роботи

1. Попередні дослідження.
2. Загальний регламент про захист даних.

4. Зміст роботи

1. Вивчитипринципи роботи цибулевої маршрутизації.
2. Вивчити механізми роботи практичної реалізації цибулевої маршрутизації під назвою Tor.
3. Проаналізувати існуючі атаки на системуTorта способи протидії ним.
4. Вибрати категорію атак та запропонувати спосіб протидії.
5. Видібрати потрібні компоненти для реалізації програмного рішення.
6. Розробити відповідне програмне рішення та здійснити експериментальне дослідження.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Методика оцінки відповідності веб-ресурсу вимогам GDPR – презентація.

6. Дата видачі завдання 10.10.2018

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	10.10.2018	
2	Збір інформації	01.02.2019	
3	Дослідження предметної області та існуючих рішень	01.04.2019	
4	Розробка плану роботи	15.04.2019	
5	Побудова опитувального листа	09.05.2019	
6	Проведення дослідження програмного рішення	16.05.2019	
7	Оцінка результатів	23.05.2019	
8	Оформлення дипломної роботи	26.05.2019	
9	Отримання допуску до захисту	28.05.2019	

Студента _____ Бурдело Є.В.
(підпис) (ініціали, прізвище)

Науковий керівник роботи _____ Стьопочкіна І.В.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Дипломна робота має обсяг 76 сторінок, містить 9 таблиць та 10 рисунків, а також 10 бібліографічних джерел.

Актуальною науковою тенденцією є методика оцінки відповідності веб-ресурсу вимогам GDPR. Методи, що використовуються у даній роботі, дозволяють проводити оцінку типового веб-ресурсу, яку можна застосовувати для ресурсів з різною метою обробки персональних даних користувачів. Тому це актуально для як для володільців веб-ресурсів, так і для власників компаній, що мають власні сайти.

Об’єктом дослідженняє оцінка забезпечення захищеності персональних даних.

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

Метою роботи є дослідження методів встановлення відповідності GDPR і створення універсального опитувального листа для оцінки відповідності вимогам регламенту для веб-ресурсів.

Дана робота містить опис основних вимог GDPR та огляд статей Регламенту. У ході роботи запропонованно методику оцінки відповідності веб-ресурсу вимогам GDPR. Запропоновану методику можна використовувати для перевірки веб-ресурсу на наявність відповідності регламенту та пошуку проблемних компонентів системи, які не задовольняють вимоги закону.

Ключові слова: Загальний регламент про захист даних, персональні дані, веб-ресурс, GDPR, Європейський союз, безпека даних, методика оцінки.

ABSTRACT

The degree work consists of 76 pages, including 9 tables and 10 figures, as well as 10 bibliographic sources.

The current scientific trend is a methodology for assessing the compliance of a web resource with GDPR requirements. The methods used in this work allow us to evaluate a typical web resource that could be used for resources with a different purpose of processing personal data of users. Therefore, this is relevant for both owners of web-resources and owners of companies owning their own sites.

The object of the study is to evaluate the protection of personal data.

The subject of the study is the procedures for protecting web resources for the processing of personal data and the methodology for verifying compliance with the requirements of the GDPR.

The aim of the work is to study the methods of establishing GDPR compliance and to create a universal questionnaire to assess compliance with the requirements of the web-resource regulations.

This paper contains a description of the main requirements of the GDPR and a review of the articles of the Regulation. In the course of work, the method of assessing the conformity of a web resource with the requirements of GDPR is proposed. The proposed method can be used for cross-checking the web resource in order to comply with the rules and the search for problematic components of the system that do not meet the requirements of the law.

Key words: General Data Protection Regulation, Personal Data, Web Resource, GDPR, European Union, Data Security, Assessment Methodology.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

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 – коєфіціент важливості

ОС – операційна система

ВСТУП

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.

Актуальність роботи. 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 і завдання дослідження. Метою роботи є дослідження методів встановлення відповідності GDPR і створення методики оцінки відповідності вимогам регламенту для веб-ресурсів.

Відповідно до вищесказаного, були поставлені наступні задачі:

1) Аналіз вимог GDPR та особливостей їх застосування;
2) Виділення критеріїв відповідності GDPR;
3) Розробка методики перевірки існуючого стану захисту даних користувачів до правил GDPR, яка включає блок перевірки на основі опитувального листа, та блок перевірки на основі результатів пентесту;
4) Аналіз практичного досвіду організації роботи веб-ресурсу відповідно до GDPR;

5) Розробку рекомендацій щодо підтримки відповідності GDPR в актуальному стані.

Об'єктом дослідженняє оцінка забезпечення захищеності персональних даних.

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

Методи дослідження. Застосування методик тестування на проникнення (проект Метасплойт), аналіз літературних джерел..

Новизна одержаних результатів. Розроблено методику встановлення відповідності до вимог GDPR, яка відрізняється використанням апарату теорії нечітких множин для встановлення рівня відповідності, використанням розробленого універсального опитувального листа та тесту на проникнення з акцентом на властивості, критичні для виконання GDPR. Сформовано рекомендації для володільців веб-ресурсів.

Практичне значення одержаних результатів. Методику можна використовувати при проведенні аудиту організацій та проектуванні захисту даних згідно GDPR. Методику орієнтовано на веб-ресурси, які займаються діяльностю різного профіля із різною метою обробки персональних даних користувачів. Зокрема було проведено аудит маркет-плейсу unc.ua, складено необхідні документиі поставлено технічне завдання щодо впровадження відповідності GDPR.

1 ОБРОБКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ВІДПОВІДНО ДО GDPR

В сучасному світі доволі важливим є питання захист персональних даних. Пакет захисту даних, прийнятий у травні 2016 року, має на меті зробити Європу придатною для цифрового віку. Більше 90% європейців стверджують, що хочуть мати однакові права на захист даних в ЄС і незалежно від того, де їхні дані обробляються. Комерційні компанії, веб-ресурси, державні установи та волонтерські організації проводять роботи щодо обробки та захисту персональних даних своїх клієнтів. Захист проводиться як з допомогою організаційних, технічних сторін та створенням необхідної документації.

Основною метою цього розділу є визначення поняття персональних даних, теоретичні та юридичні моменти їх захисту, огляду існуючих рішень і досвіду провідних світових компаній та аналізом основних положень акту Загального регламенту про захист даних.

1.1 Персональні дані

Першим кроком треба визначити, що вважається персональними даними. Опираючись на текст Загального регламенту про захист даних, зазначено: персональними даними вважається будь-яка інформація, що відноситься до ідентифікованої фізичної особи (володільця даних), за якою прямо або опосередковано можна її визначити. Різні відомості, зібрані разом, можуть призвести до ідентифікації конкретної особи, а також становитимуть її особисту інформацію.

Персональні дані, які були деідентифіковані, зашифровані або псевдонімізовані, але можуть бути використані для повторної ідентифікації особи, залишаються ПД, вважаються приватною інформацією і підпадають під сферу дії закону.[1]

Персональні дані, які були анонімні таким чином, що особа не є або більше не може бути ідентифікована, більше не вважаються ПД. Щоб дані були анонімними, анонімізація повинна бути незворотною.

До персональних даних відносяться:

1. ПІБ (прізвіще, ім'я, по батькові);
2. Домашню адресу;
3. Адреса електронної пошти, наприклад name.surname@namecompany.com;
4. Номер ID-картки;
5. Дані про місцезнаходження (наприклад, дані про місцезнаходження на смартфоні);
6. Адреса Інтернет-протоколу (IP);
7. Ідентифікатор cookie;
8. Ідентифікатор реклами вашого телефону;
9. Дані веб-портрету;
10. Дані особи, що знаходяться в лікарні;
11. Один або декілька факторів, характерних для фізичної, генетичної, розумової, економічної, культурної і соціальної ідентичності цієї фізичної особи.

Важливо зауважити, що існують деякі типи даних, що відносяться до категорії особливих або конфіденційних персональних даних. Це інформація, що містить:

1. расове або етнічне походження;
2. політичні погляди;
3. релігійні або філософські переконання особи;
4. членство в профспілках.

Окрім того, до цієї групи відносяться генетичні та біометричні дані, які можуть бути використані для ідентифікації фізичної особи, дані про стан здоров’я особи, відомості, що стосуються сексуального життя або орієнтації.

Не вважається персональними даними:

1. Реєстраційний номер компанії;

2. Адреса електронної пошти, наприклад info@namecompany.ua;
3. Анонімні дані.

Поняття «персональні дані» у розумінні GDPR охоплює значно більший обсяг інформації, ніж здається на перший погляд. Тому у контексті Регламенту завжди потрібно керуватися правилом: «У разі наявності будь-яких сумнівів щодо того, чи є інформація ПД, – її необхідно вважати ПД та обробляти відповідно до вимог GDPR».

1.2 На кого розповсюджується дія регламенту

За кордонами ЄС виконувати GDPR повинні будуть в першу чергу:[1]

1. Додатки, хмарні сервіси, що працюють з європейськими персональними даними;
2. Аутсорсингові компанії в IT-галузі;
3. Інтернет-магазини, соціальні мережі;
4. Веб-додатки, що оброблюють дані користувачів з ЄС;
5. Готелі, хостели;
6. Банки, медичні компанії, організатори публічних заходів.

Отже, власникам однієї із таких організацій бути необхідним переконатися у відповідності всім вимогам Регламенту.

У разі недотримання вимог GDPR – втрата європейських клієнтів, постачальників, ринків та ризик штрафів за порушення норми до 20 млн євро або 2-4% від річного обороту порушника. Також існує ймовірність блокування веб-ресурсів на території ЄС.

1.3 Як визначити необхідність впровадження вимог GDPR

Для того, аби визначити, чи потрібно компанії/веб-ресурсу відповідати вимогам GDPR скористуємося рисунком 1.1.

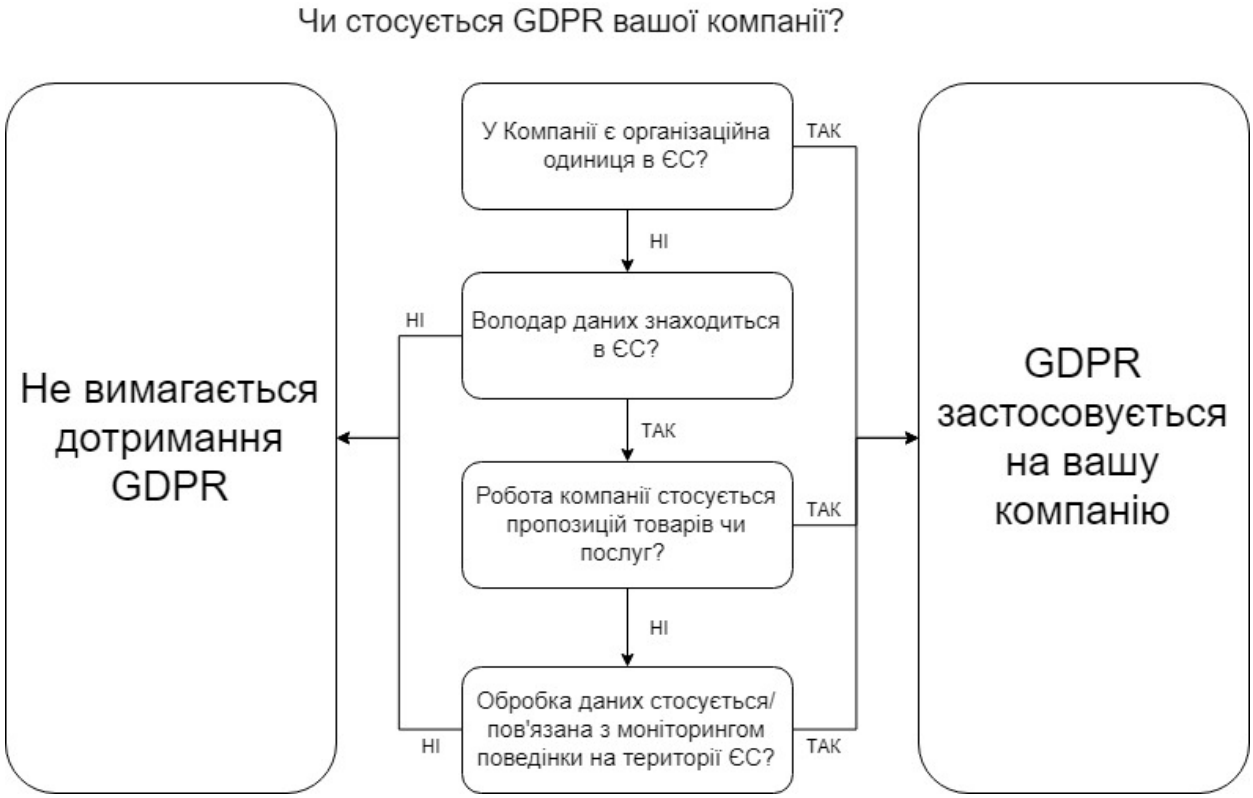

Рисунок 1.1 – Яким компаніям необхідно відповідати GDPR

1.4 Предмет і завдання GDPR

Як сказано у статті 1 «Про предмет та цілі» GDPR[1]:

1. Цей Регламент встановлює правила, що стосуються захисту фізичних осіб стосовно обробки персональних даних та правил, що стосуються вільного переміщення персональних даних;
2. Цей Регламент захищає основні права і свободи фізичних осіб, зокрема їхнє право на захист персональних даних;
3. Вільний рух персональних даних в межах ЄС не обмежується і не забороняється з причин, пов'язаних з захистом фізичних осіб у зв'язку з обробкою персональних даних.

Країни ЄС створили національні органи, відповідальні за захист персональних даних відповідно до статті 8(3) Хартії основних прав ЄС.

Можна зробити висновок, що основним завданням Регламенту є не обмеження використання персональних даних, а їх захист і вільне переміщення. Європейський Союз зацікавлений у тому, аби його мешканці були впевненні, що жодна фізична установа і веб-ресурс нікому не передасть їхні дані і не використає без відома володільця.

1.5 Принципи обробки даних по GDPR

В 5 статті «Принципи, що стосуються персональних даних» GDPR зазначено, що загальний підхід обробки ПД викладений у основних принципах[1]:

1. *Законність, справедливість та прозорість*

   Персональні дані повинні оброблятися саме так. Будь-яку інформацію про мету, методи та обсяги обробки персональних даних мається викладати максимально доступно та просто.

2. *Обмеження застосування*

   Особисті дані повинні збиратися та використовуватись виключно з метою, що була заявлена компанією (або веб-ресурсом).

3. *Мінімізація даних*

   Забороняється збирати персональні дані в більшому обсязі, ніж той, що потрібен для досягнення мети обробки. Лише цільові дані, необхідні для роботи з ресурсом.

4. *Точність*

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

5. *Обмеження зберігання*

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

6. *Цілісність та конфіденційність*

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

1.6 Основні вимоги GDPR

Опираючись на матеріали регламенту, можна виділити основні теми вимог GDPR:[1]

- *Контроль даних*

GDPR планує, що організації будуть контролювати свої дані, щоб забезпечити доступ до них та обробку їх авторизованими користувачами лише за необхідності. Вимоги до контролю наведені у статтях 5, 25 та 32 GDPR.
Відповідно до вимог GDPR організації забов`язані:

-передавати дані виключно авторизованим користувачам;

-забезпечити точність та цілісність даних;

-мінімізувати розкриття особистості суб'єкта;

-застосовувати заходи із безпеки використання даних.

Шифрування – метод, при якому дані знаходяться в нечитабельному вигляді, якщо тільки користувач, або процес не надасть відповідний ключ для розшифрування. Відповідно до GDPR, цей простий метод може забезпечити доступ до персональних даних тільки авторизованим особам, а також контролювати час (термін), протягом якого цей доступ може бути здійснений.

Багатофакторна автентифікація – метод, що забезпечує надійну авторизацію об'єкта, який здійснює обробку конфіденційних даних, а також значно зменшує ризики доступу неавторизованих користувачів до персональних даних, тим самим не допускаючи їх використання. Прикладом багатофакторної

автентифікації може бути підтвердження реєстрації через електронну пошту або номер телефону.

- *Безпека даних*

GDPR гарантує конфіденційність. Обов'язки з захисту інформації регулюються статтями 6, 25, 28 та 32. Для збереження приватності суб’єкта організаціям необхідно:

-застосувати захист ПД за проектом та за замовчуванням;

-включити безпеку до зобов’язань за контрактом з партнерами і постачальниками послуг;

-використовувати шифрування або псевдонімізацію;

-застосувати заходи безпеки, що стосуються оцінки ризиків;

-вжити заходів, якщо дані зберігаються для подальшої обробки.

GDPR робить акцент на шифрування, як на основну вимогу безпеки даних. Крім того, організаціям необхідно провести оцінку ризиків, а потім прийняти заходи, що пом'якшують ризики, які вони виявлять. Оскільки жодна організація не може повністю визначити або передбачити всі ризики для своїх даних, і жоден підхід до периметра безпеки не є надійним, організації повинні шифрувати свої дані і ПД користувачів, для того щоб забезпечити відповідність до GDPR. Завдяки шифруванню неважливо, чи є порушення – дані будуть належно захищені.

- *Право видалення*

Після того, як дані вже зібрані, володільці даних та довірені суб’єкти все одно мають певний контроль над своїми ПД. "Право на видалення" розглядається у статтях 17 та 28. GDPR вимагає від організацій повністю знищити дані з усіх сховищ в разі, якщо:

-користувач відклив свої дані;

-партнерська організація вимагає видалення особистих даних своїх користувачів, які були наданні для обробки;

-термін дії угоди про використання ПД закінчився.

Згідно цієї норми, передбачаються випадки, коли організація повинна буде забезпечити повне видалення персональних даних своїх користувачів. Це дуже складна вимога, тому що, навіть після видалення, дані все-одно зберігаються на магнітних носіях інформації.

Але щоб повністю відповісти нормі, організації можуть шифрувати дані, а потім видалити тільки ключ шифрування. Цей метод перетворює дані в повністю і назавжди нечитабельний масив інформації.

- *Профілактика ризиків та комплексна перевірка*

Організації повинні самостійно оцінювати ризики, що пов’язані з конфіденційністю та безпекою даних, а також демонструвати, що вони вживають всіх відповідних заходів з урахуванням зроблених ними висновків. Ці обов'язки викладені у статтях 2, 24 та 28. З метою зменшення ризиків та виконання комплексної перевірки організація зобов’язана:

-виконати повну оцінку ризиків;

-застосувати заходи для забезпечення та демонстрації відповідності;

-активно сприяти партнерам та клієнтам у досягненні відповідності;

-демонструвати повний контроль над наданими їм даними.

Коли організація укладає контракти з партнером чи стороннім сервісом, вони не мають відмовляються від відповідальності за безпеку даних. Фактично, організаціям буде покладено договірне зобов'язання підтримувати один одного стосовно безпеки та мінімізації ризиків витоку чи пошкодження даних.

Оскільки шифрування забезпечує безпеку безпосередньо до даних, то організації-партнери залишаються відповідними даній вимозі, оскільки захист гарантується незалежно від того на чиїй стороні зараз знаходяться ПД.

- *Повідомлення про витік даних*

Якщо порушення безпеки загрожує правам та конфіденційності володільця чи суб'єкта даних, організаціям необхідно повідомити клієнтів та їх наглядовий орган. Обов'язки щодо повідомлення про порушення викладені у статтях 33 та 34. В рамках GDPR організації зобов'язані:

-повідомити свій наглядовий орган протягом 72 годин;

-описати наслідки порушення безпеки даних;

-повідомити про порушення безпосередньо володільців чи суб'єктів даних.

Якщо у результаті витоку інформації розкриваються незахищені дані, організація зобов’язана повідомити місцевий орган нагляду та клієнта, що постраждав. Проте у випадку, якщо дані зашифровані та використовуються найкращі методи управління ключами шифрування, організація позбувається потреби у таких повідомленнях.

1.7 Сфера дії GDPR

Розглядаючи питання можливості застосування норм Загального регламенту про захисту даних до українських веб-ресурсів, необхідно здійснити ряд заходів, які можуть стати визначальними в процесі прийняття правильного рішення. Разом з цим, варто враховувати особливості роз’яснень, які надаються відповідними європейськими органами.

В листопаді 2018 року, Європейська Рада Захисту Даних (EDPB) розробила та оприлюднила Роз’яснення щодо впровадження норм GDPR щодо принципу територіального застосування (Guidelines 3/2018on the territorial scope of the GDPR).[1]

Основною метою була можливість дослідити та по’яснити особливості застосування норм GDPR до компаній та веб-ресурсів, які знаходяться за межами ЄС.

Так, наприклад, ст. 3 GDPR зазначається, що для можливості визначення кола суб’єктів, до яких будуть застосовуватися положення Регламенту, необхідно застосовувати підхід, який ґрунтується двох основних критеріях:

- Критерій місце територіального знаходження;
- Критерій цільового спрямування діяльності.

Визначення меж територіального застосування GDPR повинне здійснюватися виключно в контексті того, що норми нового Регламенту можуть

бути застосовані не тільки до суб'єктів, які знаходяться на території ЄС або Європейської Економічної Зони, як це було відповідно до вимог Директиви 95/46/ЕС, а й до суб'єктів, які знаходяться на території всього світу. Потрібно мати на увазі, що коли застосовується один із вище згаданих критеріїв, діяльність суб'єкта повинна бути проаналізована дуже ретельно.

Коли організація визнає факт того, що вона зобов'язана діяти у відповідності з вимогами Регламенту, то неважливо в якому статусі по відношенню до оброблюваних ПД вона перебуває: чи то в статусі обробника, чи то в статусі контролера. Положення Регламенту будуть застосовані до компанії в тій мірі, як це визначено Регламентом по відношенню до кожної із ролей.

Важливим залишається питання щодо необхідності призначення представника організації на території ЄС, коли мова йде про застосування до діяльності організації критерію цільового спрямування.

Отже, необхідно чітко визначити, у яких випадках українські організації та веб-ресурси повинні діяти у відповідності до вимог GDPR та в яких випадках виникає необхідність призначення представника на території ЄС.

Пункт 1 Статті 3 GDPR передбачає, що Регламент застосовується до обробки персональних даних в контексті діяльності осідка контролера або обробника в ЄС незалежно від того, чи відбувається власне опрацювання в межах ЄС чи ні.

Відповідно, розглядаючи питання застосування норм GDPR через призму використання критерію місцезнаходження, потрібно зрозуміти, що ж таке осідок та як цей критерій може стосуватися українського бізнесу.

Під осідком, в розумінні пункту 22 частини Загального регламенту про захисту даних, слід розуміти стабільно діюче утворення на території ЄС, при цьому, юридична форма такого утворення (представництво, дочірня компанія у формі окремої юридичної особи чи інше) не відіграє жодної ролі.

Тобто, якщо утворення, яке пов'язане з контролером або обробником, проявляє активність на території ЄС або веб-ресурсом користуються особи з ЄС і їх ПД оброблюються (навіть cookies) , то в такому випадку слід вважати, що

відповідний контролер чи обробник мають осідок на території Європейського Союзу.

Факт наявності осідку української компанії(організації) на території ЄС – це фактор, який визначає обов'язок української компанії організувати свою діяльність та діяльність свого осідку, яка стосується обробки ПД, у відповідності до вимог Регламенту.

1.8 Світовий досвід штрафів

В Австрії, місцевий контролюючий орган розпочав провадження проти австрійського підприємства, яке навпроти свого офісу розмістило камеру зовнішнього відеоспостереження. Основною проблемою став той факт, що камера, яка не була промаркована належним чином, окрім приміщення офісу, захоплювала ще й значну частину тротуару, яким рухалися перехожі, тим самим спричиняючи порушення вимог GDPR та місцевого законодавства.

Порушення виявилося в тому, що незаконним чином здійснювався збір та обробка персональних даних перехожих, які пересувалися тротуаром. Штраф, який був застосований до підприємства склав 4000 Євро.

Висновок: розміщуючи камери відеоспостереження в публічних місцях, необхідно інформувати населення про наявність камери та про здійснення відеозйомки, а також аргументувати необхідність її здійснення.

Португальський контролюючий орган (CNPD) наклав штраф за порушення GDPR на місцеву клініку.

Порушення виявлялося в тому, що працівники клініки, зокрема, але не виключно, лікарі, дієтологи та психологи мали доступ до ПД пацієнтів через фальшиві облікові записи. Так як дане порушення стосувалося незаконного надання доступу до чутливих даних, CNPD вирішив накласти штраф в розмірі 400 000 Євро.

Висновок: 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 1

В цьому розділі були розглянуті основні статті Загального регламенту про захист даних, проаналізовано його основні вимоги положень актів. Було визначенно поняття персональних даних, теоретичні та юридичні моменти їх захисту. Наведено приклади штрафів, які були накладені на Європейські організації.

Аналізуючи практику застосування штрафних санкцій за порушення GDPR, потрібно зауважити на тому, що контролюючими органами накладаються штрафи різних розмірів, залежно від вчиненого правопорушення. Можна спостерігати, що штрафи у більших розмірах накладаються в тих випадках, коли порушення стосуються або великих об'ємів ПД, або чутливих персональних даних.

Головне, на що потрібно звернути увагу - до відповідальності можуть бути притягнуті як компанії з території ЄС, так і компанії, які зареєстровані поза межами ЄС, про що яскраво свідчить справа, яка стосується притягнення до відповідальності канадської компанії AggregateIQ.

Отже, адаптуючи свій бізнес під вимоги General Data Protection Regulation не можна забувати, що ризик застосування штрафних санкцій залежить виключно від рівня відповідальності, з якою організація підходить до вирішення даного питання. Не можна імітувати відповідність вимогам Регламенту. Власникам веб-ресурсів необхідно проводити організаційні та технічні міри, необхідні для відповідності вимогам GDPR, опису яких буде присвячений наступний розділ.

2 ОРГАНІЗАЦІЙНІ ТА ТЕХНІЧНІ КРОКИ, ПІДГОТОВКА ДОКУМЕНТІВ, ЯКІ НЕОБХІДНІ ДЛЯ ВІДПОВІДНОСТІ ВИМОГАМ GDPR

Основною метою цього розділу є огляд методики по встановленню відповідності до Загального Регламенту Захисту Даних, опис організаційних та технічних заходів, створення документації, яка необхідна для роботи веб-ресурсу. Створення універсальної моделі порушника та моделі загроз для веб-ресурса.

2.1 Практичні кроки встановлення відповідності до вимог GDPR

Одразу слід зазначити, що забезпечення GDPR compliance – це складний процес, який потребує співпраці великої кількості людей – перш за все, менеджменту компанії, юристів та технічних фахівців.

Першим кроком варто зафіксувати поточний стан системи. На цій стадії необхідно провести аналіз всіх бізнес-процесів веб-ресурса з метою виявлення конкретних процедур обробки ПД, всі об’єкти, які залучаються до обробки, порядок взаємодії веб-ресурсу з такими особами.

Результатом є складання Initial Data Mapping – своєрідної «карти» руху ПД, яка наочно фіксує фактичні умови їх обробки. Цей документ забезпечує розуміння загальних алгоритмів роботи компанії з ПД на вихідній стадії. Необхідно зобразити всі компоненти ресурса і їх основну мету, описати сценарій дії. Приклад декомпонізації роботи веб-ресурса зображено на наступній сторінці на рисунку 2.1 та рисунку 2.2.

Рисунок 2.1 – Діаграмма потоку даних на веб-ресурсі рівня 0.

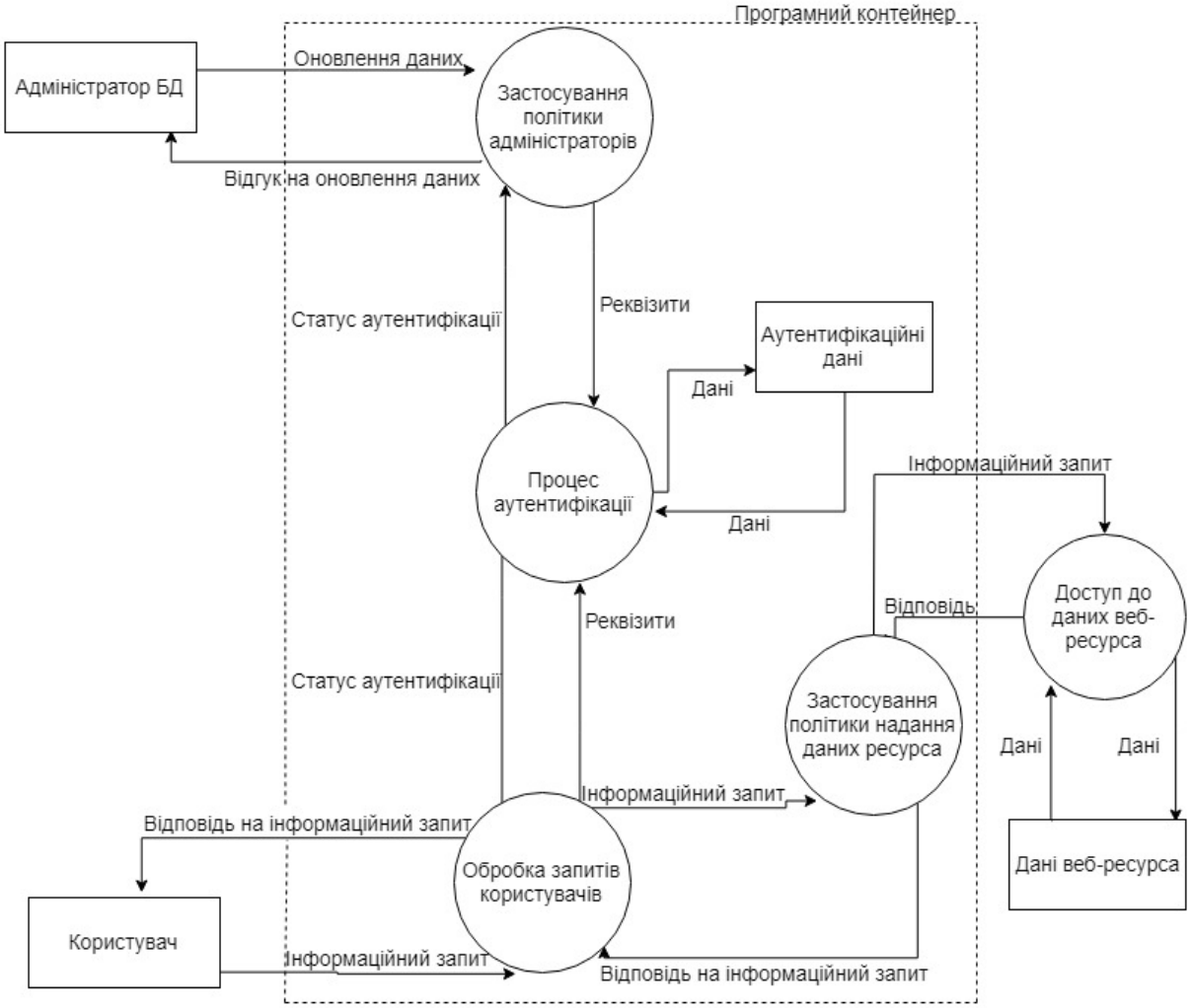

Рисунок 2.2 – діаграма потоку даних на веб-ресурсі рівня 1.

Отже, список основних компонентів типового веб-ресурса має такий вигляд:

1. Адміністратор БД
2. Користувач
3. Інтерфейс користувача
4. Інтерфейс оновлення даних на сервері
5. Сервер, на якому знаходиться веб-ресурс
6. Дані аутентифікації
7. Бізнес-логіка роботи с даними ресурса
8. Сервер БД
9. Дані ресурса
10. Бізнес-логіка інтерфейса оновлення даних ресурса

Другим кроком треба оцінити цей самий стан. Отримавши розуміння поточних алгоритмів обробки ПД, необхідно визначити, що слід змінити в таких алгоритмах для забезпечення відповідності вимогам Регламенту. Першочергово необхідно проаналізувати:

- політику конфіденційності щодо її відповідності вимогам GDPR;
- форму, у якій суб’єкту даних повідомляється про обробку його ПД;
- положень про конфіденційність в укладених договорах;
- інші документи внутрішнього та публічного характеру.

У разі, якщо обробка ПД імовірно призведе до виникнення високого ризику для прав та свобод суб’єктів даних, організація зобов’язана провести оцінку впливу на захист даних (Data Protection Impact Assessment).

Результатом данного кроку є визначення компанією різниці (Gap Assessment) між поточним станом своєї діяльності та тим станом, якого вона повинна досягти після впровадження всіх необхідних заходів відповідно до вимог Регламенту. Gap Assessment є своєрідною інструкцією на шляху досягнення GDPR compliance.

Третім кроком необхідно розробити документи. Це завжди основна стадія, від правильності та ефективності реалізації якої залежить відповідність компанії вимогам GDPR. Умовно всі документи можна поділити на політики, процедури та інші документи.

Політики визначають основні засади, якими компанія керується в процесі обробки ПД. Прикладами політик є:

- Privacy Policy – документ для сповіщення суб'єктів даних про порядок обробки компанією їх ПД;
- Cookies Policy – документ, у якому зазначено, які саме файли cookies використовує веб-ресурс. Також у користувача має бути можливість вибрати, які саме файли може використовувати ресурс;
- GDPR Controller/Processor Agreement Policy – політика, яка визначає порядок укладення договорів між компанією і обробниками персональних даних та вказує на ключові моменти таких договорів.

Процедури, у свою чергу, розкривають офіційний порядок реалізації компанією юридично значимих дій у сфері обробки ПД. Вони відображають своєрідку інструкцію, якої компанія буде дотримуватися в тому чи іншому випадку. Прикладами процедур є:

- Privacy Notice Procedure – процедура повідомлення суб'єктів даних про порядок та особливості обробки їх ПД;
- Data Subject Request Procedure & Complaints Procedure – порядок дій компанії, у разі звернення суб'єкта даних із скаргою чи запитом на реалізацію прав, підкріплених Регламентом.

Інші документи розробляються компанією для забезпечення відповідності спеціальним вимогам GDPR. Наприклад:

- Preparation Project Plan – визначає, які заходи та коли вводяться компанією для досягнення compliance;
- Roles and Responsibilities – закріплює обов'язки менеджменту компанії та основних категорій працівників в сфері обробки персональних даних.

Вище наведено лише невелику основну частину документів, які необхідні для забезпечення відповідності вимогам Регламенту. Конкретний комплект документів та їх зміст повинен визначатися для кожного веб-ресурса окремо з урахуванням специфіки їх бізнес-процесів.

На жаль, достатньо поширеною серед українських компаній є імітація GDPR. Вона виникає, якщо компанія розробляє виключно основні публічні документи, а саме – Privacy Policy та Privacy Notice, і цим її підготовка вичерпується. Privacy Policy необхідна для відповідності вимогам статей 24 та 32 Регламенту, а Privacy Notice відповідає вимогам статей 13 та 14 Регламенту. GDPR імітація залишає поза увагою решту обов'язкових до виконання вимог Регламенту.

Володільці веб-ресурсів повинні не лише розробити необхідні документи, а й забезпечити їх реалізацію та дотримання у бізнес-процесах. Контролюючі органи при розгляді питання щодо відповідності компанії вимогам GDPR беруть до уваги реальний порядок обробки ПД користувачів, а не теоретичні моделі.

На цій стадії компанія зобов'язана призначити свого представника (representative) на території ЄС, де перебуває більшість суб'єктів, чиї ПД обробляються. Для цього не обов'язково створювати філію чи укладати трудовий договір з працівником в ЄС, достатнім буде укладання цивільно-правового договору з представником.

Забезпечення відповідності компанії вимогам GDPR – це не одноразова процедура. Після розробки документів та впровадження необхідних організаційних та технічних заходів, компанія зобов'язана:

- підтримувати відповідність наявних необхідних документів та заходів постійним змінам законодавства;
- фіксувати реальні процеси та події, які мають місце під час обробки ПД;
- проводити періодичний аудит безпеки процесів обробки ПД;
- проводити навчання співробітників, які мають доступ до ПД, щодо питань захисту даних та ІБ.

Таким чином, забезпечення відповідності українських веб-ресурсів вимогам GDPR вже перетворилося з теоретичної ідеї на реальну умову для ведення успішного бізнесу в ЄС та роботи веб-ресурсу з користувачами з Європи. Інакше, його можуть просто заблокувати на території ЄС.

2.2 Організаційні заходи, необхідні для відповідності GDPR

Задля того, аби застережитися від ризиків, зв’язаних з GDPR, компаніям необхідно виконати декілька кроків:

- Провести аудит даних, що оброблюються: які дані оброблюються, з якою метою, час зберігання, методи захисту, можливість видалення клієнтом персональної інформації;
- Продумати юридичне обгрунтування для обробки тих чи інших даних: які дані і для чого збираються. Наприклад, якщо компанія виконує візову підтримку, їм необхідно оброблювати паспортні дані клієнта. Збирати дані можна лише із підтвердження дозволу володільця даних;
- Створити політику конфеденційності: чітку і зрозумілу для користувачів;
- Повідомляти користувачів про обробку їх даних і отримувати згоду;
- Створити криптографічні засоби захисту даних: використовувати лише захищені сервера;
- Створити посаду Data protection officer: за умови, якщо оброблюються великі об’єми ПД користувачів;
- Вся документація має бути переведена на мову країни, в якій здійснюється робота компанії.

2.2.1 Політика конфеденційності

Перш за все, веб-ресурс, який збирає та використовує ПД користувачів, зазвичай публікує Політику конфеденційності. Цей документ необхідний задля

того, аби проінформувати користувача про те, як оброблюються і для чого в подальшому будуть використовуватися його дані. Раніше цей документ мав стандартні розмиті положення і розміщався на сайті компанії в тих місцях, де його зазвичай ніхто не шукати не буде.

Зараз компанія має переробити Політику конфеденційності згідно вимогам Загального Регламенту по захисту персональних даних. Необхідно обов'язково зробити можливість згоди на обробку персональних даних, проінформувати користувача про права суб'єкта даних та повідомити про правила трансграничної передачі даних.

Що має зробити компанія в Політиці конфеденційносці, аби відповідати вимогам:

1. *Визначити контролера інформації і повідомити про це користувачу*;

   Повідомляйте користува, чи є ви контролером інформації. Тобто персоною, яка я відповідальною за всі дії, які будуть в подальшому зроблені з даними користувача. Наприклад:

   ТОВ «UNC» надає Користувачеві можливість зареєструватися на сайті і отримати доступ до інформаційних і технологічних ресурсів сайту. Адміністація Unc.ua контролює спосіб і порядок збору персональної інформації користувачів, а також зберігає і використовує їх. ТОВ «UNC» вважається контролером інформації, на нього поширюються права і обов'язки, що прописані в Регламенті для контролерів інформації. Для того, аби зв'язатися з нами в будь яких час: admin@unc.ua

2. *Вказати контактні дані оброблювача даних;*

   Цей пункт можна не вказувати лише за умови, якщо компанія є і контролером, і оброблювачем даних, адже текст буде співпадати. Але, якщо компанія передає дані третій особі для зберігання або обробки – пункт є обов'язковим і має такий вигляд:

   ТОВ «UNC» передає інформацію для зберігання ТОВ «LegalHub». ТОВ «LegalHub» є оброблювачем інформації, на нього поширюються всі права та обов'язки, передбачені Регламентом для оброблювачів інформації. Ви

можете зв’язатися з ними зручним для Вас способом: телефон, електронна пошта.

3. *Вказати предмет, мету та час, на протязі якого дані будуть оброблюватися (пункт 5 GDPR);*

   Компанія має визначити лише ті дані, які необхідні їй задля реалізації мети. Обов’язково необхідно вказати користувачу, які саме дані і для чого використовуються. Також необхідно вказати, які саме наслідки ненадання тих чи інших даних.

   Наприклад:

   ТОВ «UNC» збирає Ваші персональні дані (ім’я, прізвище, по-батькові, номер телефона, адреса електронної пошти) з метою подальшого зв’язку та надання цієї інформації Вашим клієнтам. Ваші дані зберігаються на сервері ТОВ «LegalHub» напротязі 6 місяців з моменту надання даних з метою надання інформації клієнтам торгівельного майданчика Unc.ua для подальшого зв’язку з Вами, як з продавцем. У разі ненадання даних подальша можливість використання торгівельного майданчика, як продавця, буде неможлива.

4. *Вказати дані і обов’язки Data Protection Officer (DPO);*

   Ця посада не є обов’язковою. Але, за наявності, необхідно вказати її користувачеві, дані якого оброблюються.

   Наприклад:

   Data Protection Officer – особа, яка є відповідальною за зберігання, обробку та подальше видалення персональної інформації про користувачів торгівельного майданчика unc.ua. Для того, аби зв’язатися с DPO, Ви маєте можливість обрати зручний для Вас метод: телефон, електронна пошта.

5. *Прописати всі права володільця інформації (пункти 15 — 18 GDPR);*

   Необхідно виділити окремим пунктом права володільця інформації, а саме: право доступа до власних персональних даних, право бути проінформованим, право на обмеження обровки та використання даних,

право на видалення даних, право на внесення змін до персональної інформації.

Наприклад:

В будь-який час Ви маєте право змінити чи видалити свої персональні дані. Для цього необхідно написати відповідальному за обробку даних на електронну скриньку і на протязі 48 годин ваші дані будуть видалені.

6. *Описати трансграничну передачу даних (пункт 45 GDPR);*

   Необхідно зазначити, куди передається інформація і як буде використана третіми країнами.

   Наприклад:

   Вся персональна інформація користувачів зберігається на сервері, який розміщенний в Україні і має надійний ступінь захисту. Передача даних в треті країни не передбачена.

7. *Отримати від володільця інформації згоду на обробку його ПД;*

   Користувач обов'язково має підтвердити згоду на обробку персональних даних.

   Наприклад:

   Створити чек-бокс, на якому користувач має поставити галочку підтвердження. Також не буде зайвим створити капчу для того, аби уникнути випадкового підтверження.

Політика конфеденційності має бути чіткою і зрозумілою. Не має необхідності робити її дуже об'ємною, треба описати всі пункти лаконічно і не публікувати зайвого. Прописувати Політику конфеденційності необхідно мовами країн, з якими взаємодіє ресурс. Розміщення на сайті також має значення: користувач має легко перейти на сторінку Політики конфеденційності, не буде зайвим візуально виділити цей пункт.

Повідомлення про конфеденційність (Privacy notice) має бути присутнім. Як було зазначено раніше, це процедура повідомлення суб'єктів даних про порядок та особливості обробки їх ПД. Користувач має отримати повну інформацію про те, для чого і які дані збираються і поставити згоду.

2.2.2 Cookie Policy

Згідно пункту 30 GDPR, інформація, що отримується за допомогою cookies, може бути використана для формування веб-портрету користувача та його ідентифікації. А отже вважається персональними даними. Тому вимагається обов'язкове підтвердження згоди з боку користувача на використання таких файлів. Раніше достатньо було звичайного баннера-повідомлення про використання cookies, але, з точки зору GDPR, цього недостатньо.[6]

Ресурс має повідомити користувача, що використовуються cookies-файли. А також має проінформувати, для чого саме і які персональні дані збирають і куди передають. Також обов'язково у користувача має бути можливість відмовитися від їх використання.

Основна мета такого підходу – зробити використання coockies більш контрольованим і зрозумілим для користувачів ресурса і, за потреби, давати можливість заборони їх використання.[8]

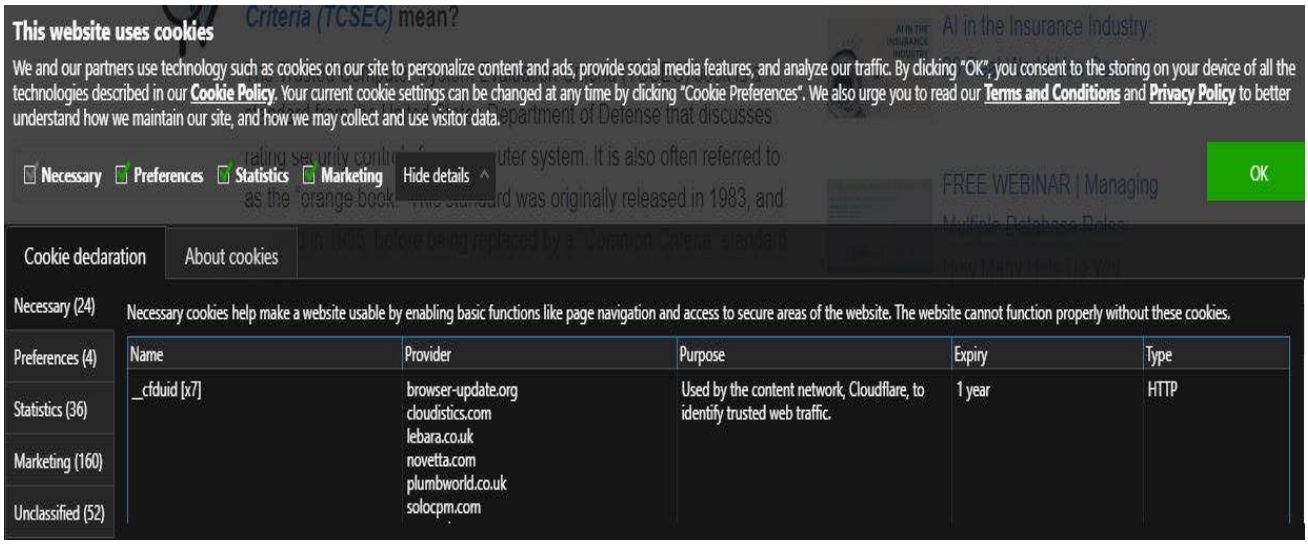

Рисунок 2.3 - Приклад повідомлення про використання cookies на сайті www.techopedia.com

На прикладі детально видно реалізацію згоди на використання cookies з можливістю користувача вибрати, на які саме файли він згоден.

2.2.3 Політика оплати

Якщо на ресурсі присутня можливість оплати послуг, необхідно також прописати політику оплати (Payment Policy), в якій має бути прописані всі можливі способи оплати і застереження з боку адміністрації ресурсу по тим чи іншим способам оплати.

2.2.4 Умови використання

Необхідно вказати, що користування веб-ресурсом (Terms of use) можливо лише особами, які досягли 16-річного віку. (Пункт 8 GDPR)

Проблема цієї вимоги полягає у тому, що майже не можливо перевірити вік користувача, адже дитина може використовувати пристрій батьків.

2.2.5 Сторінка реєстрації і особистий профіль ресурса.

Вимоги для сторінки реєстрації:

- Кількість полів для вводу персональної інформації має бути мінімальною і обґрунтованою. (Пункт 5 GDPR)
- Обов’язкове підтвердження з політикою конфеденційності і умовами використання.
- Окремий чек-бокс, якщо присутня підписка на емейл-розсилку.

Вимоги для особистого профіля:

- Користувач має право змінювати будь-яке поле своєї особистої інформації в будь-який момент. (Пункт 16 GDPR)
- Обов’язкова можливість видалення акаунта і персональної інформації. (Пункт 17 GDPR)
- Кнопка «Експорту персональних даних» (Пункт 20 GDPR)

2.3 Технічні заходи щодо впровадження GDPR

В регламенті чітко не зазначено технічних вимог, але в пункті 25 GDPR прописано, що архітектура системи має будуватися за правилом Data protection by design and by default. Це означає:

- Використання SSH;
- Впровадження двухфакторної автентифікації;
- Контроль доступу(фізичного і технічного);
- Використання сертифікованого антивіруса;
- Шифрування даних під час передачі;
- Створення зашифрованої резервної копії даних;
- Виявлення та запобігання вторгнення.

2.4 Вимоги по класам до забезпечення GDPR

Міжнародний стандарт ISO 27032 був розробленний на основі стандарта «Загальні критерії безпеки інформаційних технологій» (Common Criteria) і на його основі ставляться вимоги по классам до забезпечення GDPR. Поняття безпеки даних та їх зв'язок на веб-ресурсі, згідно стандарту виконується по схемі, що зображена на рисунку 2.4. Безпека пов'язана із захистом ПД користувачів інформаційної системи (веб-додатку) від можливих загроз.[2]

Рисунок 2.4 – Поняття безпеки даних та їх зв'язок згідно ISO 27032

2.5 Модель порушника зконцетровані на порушеннях GDPR

Під порушником в загальному вигляді можна розглядати особу або групу осіб, які в результаті навмисних або ненавмисних дій забезпечує реалізацію загроз інформаційній безпеці системи.

Таблиця 2.1 – Модель порушника типого веб-ресурса

Категорія порушника	**Кваліфікація**	**Права в системі**	**Засоби, якими володіє порушник**
Невстановлені зовнішні суб'єкти (фізичні особи)	Низька	Відсутні	Не встановлено
Технічний обслуговуючий персонал	Низька	Доступ до будь-якого мережевого вузла в разі виходу з ладу	Змова персоналу
Колишні співробітники	Середня	Відсутні	Інформація про ПЗ організації та методи захисту
Особи, які залучаються для встановлення, налагодження, монтажу та інших робіт	Середня	Доступ до мережевих вузлів, у разі проведення робіт на території КЗ	Технічні засоби і фізичний доступ до ІС
Кримінальні структури	Середня	Відсутні	Фінансова можливість найму осіб, які можуть отримати інформацію
Супровідники, розробники, постачальники	Висока	Відсутні, але можливість отримати права завдяки закладкам у ПЗ	Доступ до документації та початкового коду
Адміністратор БД	Висока	Доступ до БД, реєстрування БД, зміни налаштувань.	Спеціальний набір засобів для резервування БД без запису у реєстр
Адміністратор криптографічної підсистеми	Висока	Доступ до шифраторів, алгоритмів шифрування	Вся документація в ІС, апаратні та програмні компоненти
Зовнішні користувачі(хакери)	Висока	Відсутні	Спеціалізований набір засобів для проникнення в ІС

Модель порушника визначає:

- Категорії порушників, які можуть впливати на об’єкт обробки персональних даних;
- Мета, яку має порушник кожної категорії, засоби, якими це здійснюється;
- Сценарій, за яким діє порушник. Своєрідний алгоритм дій порушника чи групи порушників захищенності системи.

2.6 Модель загроз зконцетровані на порушеннях GDPR

При моделюванні моделі загроз в якості об’єктів, які необхідно захищати, зазвичай розглядають:

- Інформаційні системи
- Автоматизовані системи
- Бізнес-процеси
- Об’єкти інформатизації

На рисунку 2.6 зображена модель загроз для веб-ресурсів, зв’язані з порушенням ІБ.

Рисунок 2.5 – Порушення властивостей захищенності ПД веб-ресурсу

Наступним кроком буде аналіз отриманих компонентів веб-ресурса моделювання моделі загроз для об’єктів та суб’єктів системи. Необхідно дослідити кожен із компонентів на наявність можливих загроз. Для класифікації загроз використаємо методику STRIDE, в основі якої покладено 6 компонентів:

- Підміна мережевих об’єктів - ПМО
- Модифікація даних(несанкціанований доступ) - НД
- Відмова від авторства - ВА
- Розголошення інформації - РО
- Відмова в обслуговуванні - ВО
- Підвищення привілегій - ПП

Таблиця 2.2 – Можливі загрози на компоненти системи веб-ресурса

	ПМО	**НД**	**ВА**	**РІ**	**ВО**	**ПП**
Зовнішній елемент	+	-	+	-	-	-
Процес	+	+	+	+	+	+
Зберігання даних	-	+	+	+	+	-
Поток даних	-	+	-	+	+	-

Таблиця 2.3 – Модель загроз, що зосереджена на веб-ресурсі, який атакують

Загроза	**Джерело загрози**	**Імовірність + Наслідки**	**Мета (ресурс + порушення К, Ц, Д чи С)**	**Порушник**
Отримання інсайдерської інформації	Висока вартість інформації на ринку	Середня + прийнятні	БД користувачів + К	Адмін БД
Псування інформації з БД	Особисті потреби	Середня + прийнятні	БД користувачів + К	Зовнішні користувачі (хакери)
Підміна об’єктів	Особисті потреби	Середня + катастрофічні	Файловий сервер + Ц	Технічний персонал

Таблиця 2.4 – Модель загроз, зосереджена на атакуючому

Загроза	**Джерело загрози**	**Імовірність + Наслідки**	**Порушення (К,Ц,Д чи С)**	**Порушник**
DDos атака	Конкуренція	Середня + катастрофічні	К	Зовнішні користувачі (хакери)
Підміна об’єктів	Збагачення	Середня + прийнятні	Ц	Технічний персонал
Викрадення інформації з БД	Особисті потреби	Середня + прийнятні	К	Зовнішні користувачі (хакери)

Таблиця 2.5 – Модель загроз, зосереджена на програмному забезпеченні

Загроза	**Джерело загрози**	**Імовірність + Наслідки**	**Порушення (К, Ц, Д чи С)**	**Порушник**
Викрадення паролів	XSS загрозаWord Press 5.2.1	Висока + катастрофічні	К	Зовнішні користувачі (хакери)
Змінення налаштувань конфігурацій БД	Вразливість PostgreSQL	Висока + катастрофічні	Ц	Супровідники, розробники, постачальники
Відмова в обслуговуванні поштового серверу	Вразливість PostFix	Висока + катастрофічні	Д	Адміністратор криптографічної підсистеми
Аутентифікація без паролю	Вразливість Apache	Висока + катастрофічні	К	Супровідники, розробники, постачальники
Відмова в працездатності серверів	Вразливість Linux Debian	Висока + катастрофічні	Д	Технічний персонал
Викрадання особистої інформації користувачів	Вразливість Linux Debian	Висока + катастрофічні	К	Супровідники, розробники, постачальники

Висновки до розділу 2

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

Детально описано правила складання основних документів з прикладами, зокрема політика конфеденційності, 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.

На основі розділу 2 необхідно розробити методику оцінки відповідності веб-ресурса по GDPR і поради українським володільцям ресурсів, чому буде присвячений наступний розділ.

3 ОПИТУВАЛЬНИЙ ЛИСТ ПЕРЕВІРКИ ВІДПОВІДНОСТІ ВЕБ-РЕСУРСУ ВИМОГАМ GDPR

Основною метою цього розділу є створення універсального опитувального листа для веб-ресурса з різною метою опрацювання персональних даних користувачів для оцінки встановлення відповідності до Загального Регламенту Захисту Даних. Автоматизація процесу оцінки відповідності системи на основі розробленого програмного забезпечення.

Формування порад для володільців веб-ресурсів щодо аудиту відповідності GDPR, безпечному зберіганні персональних данних користувачів та роботі з клієнтами з Європейського Союзу.

3.1 Теоретична основа оцінки

Ступінь виконання визначається бальною шкалою, і одночасно враховується ступінь важливості вимог. Тоді

$$Q = \sum_{j=1}^{n} w_j B_j / n, \tag{3.1}$$

$$\sum_{j=1}^{n} w_j = 1.$$

Звідси $Q = \sum_{i=1}^{5} w_i \sum_{j=1}^{10} w_j \sum_{k=1}^{3} w_k q_{kji}$;

де n – кількість питань, B_j - Бальна шкала(1-5), W_j - ваги

Таблиця 3.1 – Відповідність між наявними видами оцінок

Бальна оцінка(N-бальна)	**Лінгвістична оцінка**	**Інтервальна оцінка**
5-відмінно	Повністю відповідає вимогам (A)	0,9-1
4-добре	Майже відповідає (B)	0,7-0,9
3-задовільно	Відповідає в основному(C)	0,5-0,7
2-незадовільно	Майже не відповідає(D)	0,3-0,5
1-цілком незадовільно	Повністю не відповідає (E)	0-0,3

Рівень захищеності веб-ресурса визначається по результатам відповідей співробітників підприємства на запропоновані методикою запитання. Попередньо визначається коефіцієнти важливості (КВ) $W_j, j = 1..n$. При цьому можно використати метод відносного ранжирування.

3.1.1 Метод відносного ранжирування

Кожні два питання порівнюються за важливістю, і експерт віддає свій голос одному з них, або може розділяти свій голос між запитаннями у певній пропорції.

Після формування КВ голоси, одержані за кожним запитанням, нормуються по формулі:

$$W_j = \frac{W_j}{\sum_{j=1}^{n} W_j} \tag{3.3}$$

таким чином, щоб виконувалось $\sum_{j=1}^{n} W_j = 1$.

Далі вводиться лінгвістична змінна «рівень відповідності», базова терм-множина якої представлена п'ятьма нечіткими термами $T = \{T_1,...,T_5\}$, які мають умовні позначки, зазначені в таблиці 3.1 – A, B, C, D, E. Діапазон зміни параметрів X_i, i=1...5 можна відобразити на універсальну множину $U = [0,4]$, а функції приналежності $\mu_i, i = 1...L$ визначити так :

$$\mu_i = \frac{1}{1 + (X_i - i + 1)^2}, i = 1...5 \tag{3.4}$$

Стандартний вигляд, який використовується в [3].

Для побудови показника відповідності, уповноважена особа веб-ресурса повинна відповісти на *n* запитань по *N*- бальній шкалі, причому значення *N* може бути різним для кожного запитання. В такому випадку використовується формула 3.5.

Далі діапазон $[\underline{X}_j, \overline{X}_j], (\underline{X}_j = 0, \overline{X}_j = N_j)$ зміни параметра $X_j^*, j = 1..n$ (кількість балів по кожному запитанню) відображається на універсальну множину $U = [0;5-1]$. Перерахунок фіксованого значення $X_j^* \in [\underline{X}_j, \overline{X}_j]$ у відповідний елемент $U_j^* \in [0;5-1]$ виконується за формулою:

$$U_j^* = (5-1)\frac{X_j^* - \underline{X}_j}{\overline{X}_j - \underline{X}_j} \tag{3.5}$$

а функції приналежності $\mu_i^j(U_j^*), i = 1...5$ нечіткого терма з номером *i* визначаються так:

$$\mu_i^j(U_j^*) = \left(\frac{1}{1+(X_i - i + 1)^2}\right)^w. \tag{3.6}$$

Після цього формуємо показник рівня відповідності:

$$\mu_S(X_j^*) = \bigvee_{i=1}^{5} \bigwedge_{j=1}^{n} \mu_i^j, \tag{3.7}$$

де $j = 1...5$ -номер терма з базової терм-множини,

$j = 1...n$ - номер запитання.

Операції $\wedge, \vee$ знаходяться мінімальне та максимальне значення відповідно по заданій множині значень функції μ_i^j .

Таблиця 3.2 – Коефіцієнти важливості блоків та результати анкетування по блоках.

№ блоку	1	2	3	4	5	6	$\sum_{i=1}^{6} Wi$	$W_i i=1...6$ $Wi/\sum Wi$	Результати по блоках в балах $X_i^*, i=1...6$
1	1/1	0,9	1,5	1,1	1,8	1,3	7,6	0,2	3,0
2	1,1	1/1	1,6	1,25	2	1,42	8,37	0,22	2,1
3	0,7	0,6	1/1	0,75	1,2	0,86	5,11	0,13	4,1
4	0,89	0,8	1,33	1/1	1,6	1,14	6,76	0,18	3,2
5	0,56	0,5	0,83	0,63	1/1	0,72	4,24	0,11	3,4
6	0,78	0,7	1,17	0,89	1,4	1/1	5,94	0,16	2,2

1. Контроль даних
2. Безпека даних
3. Право видалення
4. Профілактика ризиків та комплексна перевірка
5. Повідомлення про витік
6. Тестування на проникнення

В таблиці експерт розподіляє голоси між кожними двома відповідями, відповіді співробітника - усереднені значення, що одержані за анкетами. Ці дані є вихідними для заповнення таблиці 3.3 .

Результати оцінки, вказані в таблиці, зроблено на прикладі unc.ua.

Таблиця 3.3 – Функції приналежності та визначення рівня відповідності

№ зап.	$\mu_1^j(U_j^*)$	$\mu_2^j(U_j^*)$	$\mu_3^j(U_j^*)$	$\mu_4^j(U_j^*)$	$\mu_5^j(U_j^*)$	$\mu_6^j(U_j^*)$
1	**0,1**	**0,08**	0,35	1	0,29	0,12
2	0,16	0,45	0,98	0,48	**0,04**	**0,04**
3	0,13	0,24	**0,18**	0,55	0,99	0,51
4	0,12	0,24	0,31	0,96	0,23	0,13
5	0,24	0,39	0,41	0,91	0,34	0,25
6	0,25	0,54	0,96	**0,45**	0,09	0,09
	$\min_j \mu_1^j$	$\min_j \mu_2^j$	$\min_j \mu_3^j$	$\min_j \mu_4^j$	$\min_j \mu_5^j$	$\min_j \mu_6^j$

де μ_i, i=1..5

Далі слід обчислити $\mu_s = \max_i \mu_i$, тоді рівень відповідності вимогам має значенню відповідного терма з номером s.

$\mu_s = 0{,}45$ - отримана оцінка відповідності ресурсу unc.ua.

3.2 Принципи побудови опитувального листа

За основу взято методику комплексної оцінки системи захисту інформації веб-ресурсу, що допомагає проаналізувати ступінь виконання вимог GDPR.

Розглянемо декілька блоків показників (напрямків складання питань для опитувального листа), що характеризують систему захисту інформації та відповідності вимогам Загального регламенту про захист даних на веб-ресурсі:

- Блок показників "Вимоги";

- Блок показників "Об’єкти";
- Блок показників "Етапи".

Складемо вміст кожного з блоків.(які використовуються у якості елементів формування питань для опитувального листа)

Вимоги (B_i, i=1..5):

В якості даного блоку було прийнято основні вимоги, які передбачені Загальним регламентом про захист даних, що були детально описані раніше. До них входять:

- B_1: Контроль даних.

  Блок містить питання вимоги про контроль даних, а саме: передавання даних тільки авторизованим користувачам, точність та цілісність даних, мінімізація розкриття особистості суб’єкта, заходи безпеки використання даних;
- B_2: Безпека даних.

  Питання пов’язані із захистом даних, використання шифрування або псевдонімізації, оцінки ризиків, тощо;
- B_3: Право видалення.

  Даний блок містить питання, які прямо зв’язані із видаленням ПД користувачів у разі їх відкликання користувачем, закінчення терміну дії зберігання та інші законні підстави;
- B_4: Профілактика ризиків та комплексна перевірка.

  Блок питань має бути присвячений питанням запобігання ризиків витоку інформації, пошкодження її цілісності. Такі питання також пов’язані із комплексною перевіркою стану системи;
- B_5: Повідомлення про витік даних.

  Питання повинні висвітлити порядок дій та підстави, під час яких адміністрація веб-ресурсу має повідомляти користувачу про витік його персональних даних. У деяких випадках така інформація також повідомляється у відповідальний контролюючий орган.

Об'єкти(O_j, j=1..10):

У якості об’єктів було прийнято компоненти системи веб-ресурсу, які потребують захисту згідно вимогам GDPR. Дані елементи були складені із схеми типого веб-ресурсу і являються універсальними. А саме:

- O_1: Адміністратор БД;
- O_2: Користувач веб-ресурса;
- O_3: Інтерфейс користувача;
- O_4: Інтерфейс оновлення даних на сервері;
- O_5: Сервер, на якому знаходиться веб-ресурс;
- O_6: Дані аутентифікації;
- O_7: Бізнес-логіка роботи с даними ресурса;
- O_8: Сервер БД;
- O_9: Дані ресурса;
- O_{10}: Бізнес-логіка інтерфейса оновлення даних.

Етапи (E_k, k=1..3):

- E_1: Поточний стан системи.

  На цьому етапі необхідно зафіксувати поточний стан системи. Варто провести аналіз всіх бізнес-процесів веб-ресурса з метою виявлення конкретних процедур обробки ПД, всі об’єкти, які залучаються до обробки, порядок взаємодії веб-ресурсу з такими особами;
- E_2: Розробка документаційної бази, організаційних та технічних методів.

  Отримавши розуміння поточних алгоритмів обробки ПД, необхідно визначити, що слід змінити в таких алгоритмах для забезпечення відповідності вимогам Регламенту. На цій стадії відбувається складання необхідних документів і впровадження організаційних та технічних моментів. Відбувається оцінка вразливостей та ризиків, що були виявлені

в $E_{2.}$ Питання також стосуються етапу побудови моделі загроз і мають висвітлити правильність цієї моделі;

- E_3: Перспективні зміни (оновлення, підтримка).

  Блок питань стосується подальшого використання веб-ресурса і підтримки його в тому стані, якому буде вимагати поточний варіант Регламенту, перевірки виконання періодичного аудиту безпеки процесів обробки ПД.

В залежності від того, чи має веб-ресурс всі вказані вище компоненти (об'єкти) в своїй системі, або їх кількість більша, блок «Об'єктів» може бути розгорнутий у більш детальну сукупність конкретних показників для окремо взятого веб-ресура і відповідно, питання можуть бути задані більш детально.

Описова модель оцінки відповідності вимогам GDPR може бути представлена у вигляді поєднання блоків показників у матрицю, яка містить М елементів, де для розглянутої кількості показників у кожному із блоків.

$$M= 10*5*3=150 \text{ елементів.} \quad (3.8)$$

де М – кількість елементів, яка є добудком елементів блоків показників.

За кожним із елементів матриці закріпленно запитання і є можливість проставити оцінку, керуючись теоретичними відомостями з підрозділу 3.1. В залежності від етапу робіт можна сформувати декілька матриць, однакових за структурою, але різних за змістом.

Інколи неможливо поєднати всі три блоки в одному запитанні, тоді один із блоків не береться до уваги, запитання може стосуватись лише двох блоків, а отже в будь-якому випадку до кожного елемента матриці існує принаймі питання. Як було пораховано у формулі 3.1 , мінімальна кількість запитань – 150.

Запитання даються співробітнику, який обслуговує дану оцінювану систему. За його відповідями експерти ставлять оцінки за шкалою, що зазначена

вище. В результаті цих оцінок можна визначити оцінку відповідності веб-ресурса вимогам GDPR за однією із формул:

$$Q = \frac{\sum_{i=1}^{5}\sum_{j=1}^{10}\sum_{k=1}^{3} z_{kji}}{150}; \tag{3.9}$$

$$z_{kji} = \begin{cases} 1, q_{kji} > q_{kji}^{d}, \\ 0, q_{kji} \leq q_{kji,}^{d} \end{cases}$$

де q_{kji}^{d} – бажане значення показника якості для відповідного елемента матриці, q_{kji} – одержане за експертною оцінкою значення показника.

Для того, аби враховувати важливість кожного з елементів матриці, слід використовувати ваги. Однак зважити 150 елементів один стосовно одного досить складно. Тому використовуємо ваги для кожного з блоків, ребер трьохвимірної матриці окрема за формулою 3.3.

$$Q = \sum_{i=1}^{5} w_i \sum_{j=1}^{10} w_j \sum_{k=1}^{3} w_k q_{kji}; \tag{3.10}$$

де $\sum_{k=1}^{5} w_k = 1$; $\sum_{j=1}^{10} w_j = 1$; $\sum_{i=1}^{3} w_i = 1$, q_{kji} −оцінка відповідності на питання

Ваги елементів блоків:

W[B] = { 0.2, 0.2, 0.2, 0.2, 0.2};

W[O] = { 0.04, 0.08, 0.1, 0.2, 0.06, 0.05, 0.07, 0.05, 0.1, 0.25}; (3.11)

W[E] = { 0.2, 0.5, 0.3};

3.3 Опитувальний лист оцінки відповідності вимогам GDPR

Приведимо приклад декількох питань з опитувального листа. З повним переліком питань по кожному елементу матриці опитувального листа можна ознайомитися у Додатку А.

591 – Чи повідомляється користувачу про витік його даних?

431 – Політика конфеденційності знаходиться на видимому місці і доступна в один клік?

421 – Чи прийняв користувач умови користування веб-ресурсом?

132 – Користувач має можливість вибрати, які cookies використовувати?

192 – Чи передаються дані користувачів третім особам(наприклад для реклами) ?

191 – Чи збираються лише ті ПД , які потрібні для роботи з веб-ресурсом?

213 – Чи відбувається регулярна оцінка можливих ризиків витоку даних?

221 – Чи надавав користувач згоду на обробку персональних даних?

323 – Чи має користувач можливість запросити видалення власних ПД?

Числовий ідентифікатор являється своєрідною координатою елемента матриці, на основі якого ставиться питання. Після того, як уповноважений експерт обирає елемент, йому необхідно оцінити поточний рівень відповідності за оцінками, представленими у таблиці 3.1.

3.4 Методика проведення тестування на проникнення

Крім вимог відповідності вимогам GDPR, тестування на проникнення є критичним аспектом будь-якої безпеки веб-ресурсу. Постійно розвивається спектр загроз, викликаний зростаючою складністю методів атак. Це викликає необхідність постійного моніторингу та управління ризиками в інформаційних системах. Стаття 32 вимагає, щоб контролер і обробник здійснили відповідні технічні та організаційні заходи для забезпечення рівня безпеки, відповідного ризику, в тому числі:

- псевдоніми і шифрування особистих даних;
- здатність забезпечувати постійну конфіденційність, цілісність, доступність і відмовостійкість систем і послуг обробки;

- здатність своєчасно відновлювати доступність і доступ до персональних даних у разі фізичного або технічного інциденту;
- процес регулярного тестування, оцінки і оцінки ефективності технічних та організаційних заходів для забезпечення безпеки обробки.

Ця вимога говорить, що регулярне тестування безпеки включає в себе; Тестування на проникнення, оцінку вразливості і аудит безпеки, що є обов'язковою вимогою в рамках GDPR. Тест на проникнення зможе перевірити ефективність контролю шифрування, а також рівень конфіденційності, доступності та цілісності в системі обробки даних. Тестування на проникнення є важливою частиною відповідності вимогам GDPR, а також виявить ризики, пов'язані з витоком даних, включаючи особисті дані резидентів ЄС.

Metasploit Project — це проект сфери комп'ютерної безпеки, що надає інформацію про вразливості системи і допомагає у тестах на проникнення та розробці IDS. Варто зазначити, що приклади виконання експлоїтів виконані на базі тестового середовища [4].

Основні команди для роботи з модулями Metasploit Framework

- Пошук модуля, який потрібен – search;
- Обрати необхідний модуль – use;
- Налаштувати модуль - show options;
- Ввімкнути певну опцію – set;
- Опції RHOST – одна адреса цілі, RHOSTS – декілька;
- Запустити модуль – run.

Практичні кроки тестування:[7]

1. Виявлення цілі і постановка мети:

Перед проведенням пен-тесту необхідно поставити мету, з якою його проводимо. Використовуємо всі вразливості, які можуть бути виконані

потенційними зловмисниками, які мають фізичний доступ до серверів веб-ресурсу.

Exploit - модулі, що містять експлойти, тобто код, який використовує вразливість в системі і дозволяє виконати корисне навантаження, наприклад, переповнення буфера або обхід аутентифікації.

Таблиця 3.4 – Експлойти для використання вразливостей елементів моделі загроз, зосередженій на программному забезпечення.

Джерело загрози	Експлойт
PostgreSQL	exploit/multi/http/manage_engine_dc_pmp_sqli
WordPress 5.1.2	exploit/multi/http/wp_crop_rce
Postfix	exploit/linux/misc/gld_postfix
Apache(CVE-2009-3548)	auxiliary/scanner/http/tomcat_mgr_login exploit/multi/http/tomcat_mgr_deploy exploit/multi/http/tomcat_mgr_upload

Для детальної інформації про той чи інший експлойт можно скористатися командою «info».

2. Пошук інформації, яка необхідна для мети:

Виконується сканування вузлів системи, пошук доступних папок і файлів, визначаються імена комп'ютерів, які адмініструють систему веб-ресурса.[9]

Сканування портів

Використовуємо nmap. Стандартно сканується 1000 найпоширеніших портів. Ключи:

- -p- дозволяє сканувати всі наявні порти;
- -O визначає операційну систему;

- -sV визначає версію служб.

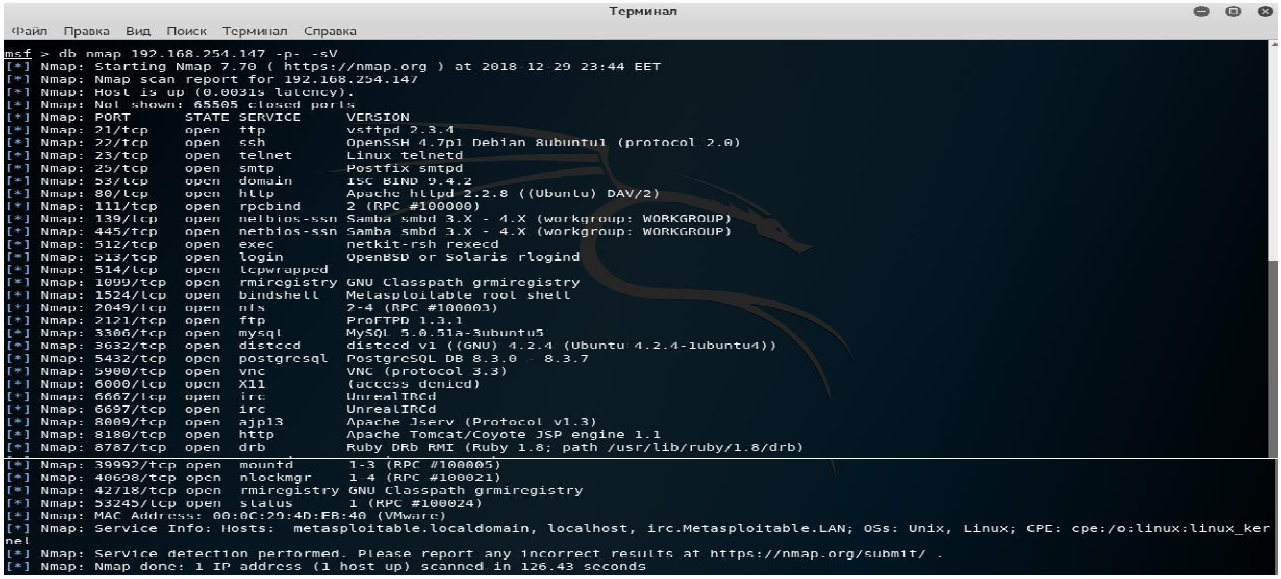

Рисунок 3.1 – Сканування портів на прикладі Metasploitable2

Пошук доступних папок і файлів

Для пошуку SMB-ресурсів скористаємося модулем auxiliary / scanner / smb / smb_enumshares.

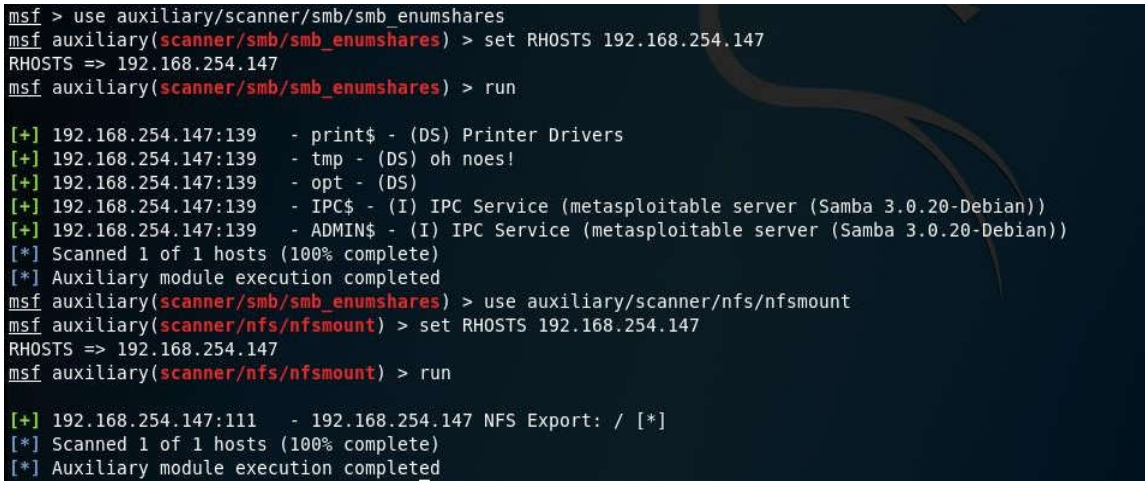

Рисунок 3.2 – Пошук доступних папок і файлів

Пошук систем керування БД

Для пошуку систем керування MS SQL використовуємо модуль auxiliary/scanner/mssql/mssql_ping. Визначаємо UDP порт 1434 і TCP-порт, по якому БД чекає підключення.

3. Виявлення вразливостей системи:

Виявлення вразливостей за версією продукту повноцінно не реалізовано в Metasploit Framework, так як для автоматизованого виявлення потенційних вразливостей в першу чергу використовуються сканери вразливостей. Проте деякі модулі експлуатації в Metasploit Framework підтримують метод check, який можна використовувати для визначення наявності уразливості до її експлуатації.

Для аналізу вразливостей підійдуть дані про версіях мережевих сервісів, отримані на попередньому етапі в ході сканування портів. Для того, аби знайти опис вразливості і експлойт, необхідно формувати пошукові запити в Google виду «сервіс версія» + vulnerability + exploit. Таким чином формується так зване CVE. Також для пошуку CVE можна скориститатися ресурсом [10].

4. Проведення атак:

Для експлуатації вразливостей в мережевих сервісах використовуються експлойти з розділу «exploit Metasploit Framework». Відповідні експлойти можна знайти за допомогою search, вказавши код CVE, назву або версію сервісу.

```
msf > search vsftpd

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command
Execution
```

Рисунок 3.3 – Приклад використання команди search

Приклад атаки підбору паролей PostgreSQL і сервер додатків ApacheTomcat, встановленим на [4]:

Pass-the-hash

Для успішної авторизації не обов’язково знати пароль, а досить лише мати хеш пароля і ім'я облікового запису. Дана вразливость може бути у будь-якої

ОС, в якій використовується протокол NTLM. Атаку pass-the-hash можна провести за допомогою модуля exploit/windows/smb/psexec.

В результаті тестування захищеності ми маємо перелік вразливостей, які можуть бути виконані зловмисниками, причому віддалено. Результатом запуску експлойтів і проведення атак є доступ до різних систем, а також інформація облікових записів.

5. Підвищення прав в системі:

Інколи є можливість підвищення привілеїв, що дає право стандартному користувачу отримати права адміністратора.

Це можливо, коли:

Користувачі, що використовують однакові паролі

Часто користувачі люблять використовувати однакові паролі на різних веб-ресурсах, тому доцільно перевіряти один раз підібрані пари логін: пароль у всіх ресурсах.

Розробники, що не видаляють з тестового середовища особисті дані

Тестові середовища дуже часто створюються шляхом відновлення з резервних копій бойових середовищ, при цьому не завжди приділяється належна увага питанням інформаційної безпеки. Так, наприклад, можуть створити обліковий запис адміністратора з легко вигадуваним паролем або не встановити критичні оновлення ОС. Отримавши доступ до тестового середовища, є можливість вивантаження ПД користувачів (логіни і хеши паролів), які відповідають тим, що використовуються в на основному веб-ресурсі.

В Metasploit Framework також є набір модулів, що дозволяють вирішувати такі завдання для розширення доступу та підвищення привілеїв:

a. пошук потрібних локальних експлойтів (post / multi / recon / local_exploit_suggester);

b. запуск кейлога (post / windows / capture / keylog_recorder);
c. збір облікових записів і хешів користувачів (post / windows / gather / credentials / credential_collector).

В результаті після виконання даного кроку може бути виявленно реальні локальні уразливості системи веб-ресурса.

6. Створення звіту тестування:

Основною частиною звіту є інформація про вразливість, яка подається в такому вигляді:

- виявлення - інформація про назву уразливості, CVE, перелік вузлів, на які може впливати.
- тестування - скріншоти і журнали, які демонструють тестування необхідної вразливості;
- ризик - до чого може привести використання вразливості;
- рекомендації - технічні і організаційні рекомендації з мінімізації можливості використання вразливості.

3.5 Рекомендації володільцям веб-ресурсів

Декілька структурованих порад володільцям веб-ресурсів, які мають на меті відповідати вимогам Загального регламенту про захист даних:

- *Зберігайте всю інформацію* про співробітників, клієнтів, постачальників структуровано і зі зручним інтерфейсом пошуку. В наші дні існує великий вибір програм для зберігання і обліку інформації. Завдяки їм ви зможете досить швидко зробити запит на пошук потрібної інформації, а також зможете продемонструвати структурований облік інформації, що зберігається, проходячи перевірку на відповідність GDPR відповідними контролюючими органами.

- *Забезпечуйте надійний захист інформації.* Питання безпеки дуже глобальні, і досить важко захистити себе від хакерських атак. Важливо зробити максимум для попередження витоків даних. Наприклад, необхідно переконатися, що антивірусні програми у вас ліцензійні і постійно оновлюються. Переконатися, що ви зможете дистанційно вийти з усіх акаунтів, щоб ніхто не зміг отримати доступ до внутрішньої інформації компанії в разі втрати робочого ноутбука. Непоганим буде прописати чіткий алгоритм дій у разі надзвичайної ситуації. А в разі розслідування на відповідність захисту ПД, ви зможете продемонструвати, що зробили все можливе для максимального збереження інформації.
- *Зберігайте тільки ту інформацію, яка дійсно необхідна.* Для мінімізації ризиків краще не зберігати те, що, можливо, коли-небудь знадобиться. Кожна одиниця інформації несе в собі додатковий ризик для компанії в разі витоку. Тому краще оперувати тільки необхідним масивом, а в майбутньому, якщо виникне необхідність, запросити у користувачів згоду на використання ПД з новою метою.
- *Оптимізуйте процес надання інформації*, яка у вас зберігається, за запитом користувача - власника ПД. Відповідно до Регламенту, ви зобов'язані протягом 1 місяця надати всю таку інформацію безкоштовно.
- *Розробіть механізм видалення особистих даних користувача* за його запитом. Всі дані будь-якої особи повинні мати опцію оперативного видалення з усіх можливих сховищ, документів, розсилок тощо. Цей процес називається «право бути забутим» і має обов’язково бути присутнім на вашому веб-ресурсі.
- *Розробіть чітку і зрозумілу форму-підтвердження*, щоб користувачі могли «активно» дати згоду. Активне згоду на обробку ПД передбачає особисту простановку відповідної позначки («чек-боксу») в електронній формі або підписання документа (якщо згода надається не онлайн) для кожної окремої мети.

- *Реалізуйте можливість швидкого припинення надходження будь-яких повідомлень* від вашого ресурсу. Якщо ви створюєте розсилки інформаційних листів, смс, дайджестів, рекламних акцій, то повинна бути опція негайної відписки від ваших листів.
- *Донесіть основну інформацію про Регламент* до своїх співробітників. Оскільки саме вони будуть оперувати даними користувачів, а за порушення штрафується компанія. Крім цього, бажано призначити відповідальну особу за дотримання вимог, які були перераховані вище.
- *Перевіряйте бази даних при їх придбанні*. Переконайтеся, що продавець правомірно зібрав інформацію, і всі, хто надав її, активно погодилися на це. Придбання даних зазвичай використовується задля всіляких маркетингових акцій.
- *Проведіть аудит веб-ресурсу на відповідність всім вимогам GDPR.* За допомогою створенного опитувального листа у володільців веб-ресурсів є можливість провести комплексну оцінку відповідності вимогам Регламенту та виправити стан системи на потрібний.

Висновки до розділу 3

В цьому розділі були описані теоретична основа оцінки відповідності веб-ресурсу вимогам GDPR, встановлені вхідні дані матриці питань опитувального листа та дані якісні загальні поради володільцям веб-ресурсів, щодо впровадження відповідності вимогам регламенту.

Окремо було наведено приклади питань опитувального листа. Також детально описано метод відносного ранжування, за яким встановлюється коефіцієнт важливості блоків питань листа.

Результат тестової оцінки unc.ua:

Відповідність веб-ресурса вимогам GDPR: 0.355180 – результат unc.ua, згідно проведенного тестового оцінювання веб-ресурса.

ВИСНОВКИ

Дана робота присвячена створенню універсальної методики оцінювання відповідності типового веб-ресурса вимогам Загального регламенту про захист даних. Було отримано ряд результатів:

1) Проведено аналіз вимог GDPR та особливостей їх застосування; зокрема:

- проаналізовано основні статті Регламенту;
- побудовані моделі загроз та порушника безпеки веб-ресурсу (табл.2.1 - 2.5);
- проаналізовано вимоги , що стосуються технічніх заходів, яких вимагає GDPR

2) На основі аналізу 1) виділено виділено основні групи вимог, обрано методику оцінки відносної важливості кожної із груп для певної установи, на основі якої виділено критерії оцінки відповідності GDPR (міра приналежності стану захищеності в організації, що аналізується, до класів Н, НС, С, ВС, В забезпечення GDPR).

3) Описано практичні дії по встановленю відповідності вимогам GDPR, приведено приклади оформлення основних політик згідно вимогам регламенту, запропоновано методику, яка включає аналіз на основі створеного опитувального листа та результатів тесту на проникнення для оцінки відповідності вимогам GDPR;

4) Проведено аналіз практичного досвіду роботи веб ресурсу, на прикладі маркет-плейсу unc.ua на основі запропонованої методики;

5) Подано практичні поради для володільців та адміністраторів веб-ресурсівщодо підтримки відповідності GDPR в актуальному стані (в частині програмних, апаратних та організаційних засобів).

Оскільки опитувальний лист містить массив питань, що охоплюють всі компоненти системи типового веб-ресурса, вимоги GDPR і рекомендовані етапи впровадження відповідностей, то можна сподіватись, що запропоновану методику оцінки можна буде використати для веб-ресурсів із різноманітною метою обробки даних та бізнес-процесами. Як перспектива, запропонована методика може бути доповнена в залежності від додаткових компонентів системи веб-ресурсу, що оцінюється.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). // Official Journal of the European Union. – 2016.
2. Технічний комітет зі стандартизації «Інформаційні технології» (ТК 20). ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT) // ДП «УкрНДНЦ». – 2018.
3. Основы теории нечетких множеств / Л. К. Конышева, Д. М. Назаров. – Санкт-Пітербург: Питер, 2011. – 192 с.
4. Project Metasploit [Електронний ресурс] // Rapid7. – 2018. – Режим доступу до ресурсу: https://metasploit.help.rapid7.com/docs/exporting-project-data.
5. Metasploitable2 [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://sourceforge.net/projects/metasploitable/.
6. Documentation for the Cookie Consent plugin [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://cookieconsent.osano.com/documentation/about-cookie-consent/.
7. Technical Guide to Information Security Testing and Assessment / K.Scarfone, M. Souppaya, A. Cody, A. Orebaugh. // Recommendations of the National Institute of Standards and Technology.
8. Как грамотно предупредить о файлах cookie на сайте [Електронний ресурс] // NetPeak. – 2018. – Режим доступу до ресурсу: https://netpeak.net/ru/blog/kak-gramotno-predupredit-o-sbore-cookie-na-sayte/
9. Vulnerability & Exploit Database [Електронний ресурс] // Rapid7 – Режим доступу до ресурсу: https://www.rapid7.com/db/.
10. CVE details [Електронний ресурс] – Режим доступу до ресурсу: https://www.cvedetails.com.

ДОДАТКИ

ДОДАТОК А

Питання опитувального листа для елементів матриці

В додатку представлений повний перелік питань опитувального листа, що відповідають кожному з елементів матриці.

Перший елемент нумерації відповідає за блок «Вимоги»

Другий елемент – за блок «Об’єкти»

Третій елемент – за блок «Етапи»

Коєфіціент Х відповідає за число «10» для зручності.

Питання блоку вимоги «Контроль даних»

111 – Чи здійснюється робота з ПД користувачів лише через локальну мережу?

112 – Чи виконується контроль доступу (технічний) до системи веб-ресурсу?

113 – Чи дотримується конфеденційність та цілісність даних?

121 – Чи було ознайомлення з усіма правилами та політиками, які представлені на ресурсі?

122 – Чи присутня вся документація і відповідає вимогам?

123 – Чи складено ТЗ із модернізації політи безпеки і cookies?

131 – Веб-ресурс попереджає про використання cookies?

132 – Користувач має можливість вибрати, які cookies використовувати?

133 – Чи є можливість змінити будь-яку інформацію в особистому профілі?

141-Чи всі поля в БД, які містять ПД користувачів є обов’язковими до заповнення?

142 – Чи має користувач можливість ознайомитися з метою збору кожного елемента даних?

143 – Заявки на відкликання даних оброблюються вчасно?

151 – Веб-ресурс використовує ssl?

152 – Чи обмежений фізичний доступ до сервера?

153 - Використовується платний, перевірений веб-хостинг?

161 – Чи кожне поле реєстрації необхідне і обгрунтоване?

162 – Ч избираются дані, які не потрібні для роботи ресурса ?

163 – Чи відбувається регулярний перегляд необхідності збору даних, що збираються?

171 – Чи є можливість не надавати ПД з поясненням, які функції веб-ресурса будуть недоступні?

172 – Чи є можливість обрати, які файли cookies може використовувати ресурс?

173 – Політика конфеденційность знаходиться на видимому місці?

181 – Чи використовується шифрування?

182 – Чи обмежений фізичний доступ до сервера?

183 – Чи присутня цілодобова підтримка безпеки даних користувачів на сервері БД?

191 – Чи збираються лише ті ПД , які потрібні для роботи з веб-ресурсом?

192 – Чи передаються дані користувачів третім особам(наприклад для реклами) ?

193 - Дані зберігаються в зашифрованному вигляді?

1X1 – Оновлення даних проводять лише з робочої машини?

1Х2 – Оновлення виконує лише уповноважена особа (Адміністратор БД)?

1Х3 – Чи виконується коррегування невірних даних користуввачів?

Питання блоку вимоги «Безпека даних»

211 – Чи ознайомлений з правилами безпечної обробки даних?

212 – Чи присутня посада DPO ?

213 – Чи відбувається регулярна оцінка можливих ризиків витоку даних?

221 – Чи надавав користувач згоду на обробку персональних даних?

222 – Чи є доступ до особистого кабінету користувача у третіх персон?

223 – Чи повідомляють про права користувачів?

231– Чи присутні спеціальні вимоги до паролів (верхній/нижній реєстр, цифра, кількість символів, тощо)?

232 – Чи є «термін дії» пароля?

233 – Оновлення паролів виконується лише з підтвердженням особи?

241 – Чи мають треті особи доступ до оновлення даних?

242 – Чи прописані правила безппечного оновлення даних?

243 – Чи проводиться регулярний перегляд запитів на оновлення даних?

251 – Чи використовується ліцензований антивірус?

252 – Чи прописані вимоги щодо безпеки сервера?

253 – Чи безпечний сервер, на якому знаходиться веб-ресурс?

261 – Чи є можливість використання «слабкого» пароля?

262 – Чи виконані всі вимоги безпеки до паролів користувачів?

263 – Чи виконується обмеження на «термін життя» пароля?

271 – Чи є доступ до всіх даних користувачів у незареєстрованих юзерів?

272 – Чи приховуються контактні дані користувачів(якщо є) для неможливості використання ботами та парсерами?

273 – Чи використовується «капча»?

281 – Результат пен-тесту сервера задовольняє вимоги безпеки?

282 – Чи використовується криптографічний захист даних (наприклад, шифрування)?

283 – Чи проводиться регулярна перевірка ПЗ тестуванням на проникнення?

291 – Чи були випадки витоку даних користувачів?

292 – Чи створена модель порушника і всіх можливих загроз для веб-ресурса?

293 – Паролі зберігаються в хешованому вигляді?

2Х1 – Чи має адміністратор доступ до паролів користувачів?

2Х2 – Зберігання ПД відбувається так, як описано в угоді користувача?

2Х3 – Чи є можливість змінити дані користувача без його відома?

Питання блоку вимоги «Право видалення»

311 – Чи ознайомлений адміністратор з правилами видалення відкликаних даних?

312 – Чи прописані правила видалення ПД?

313 – Чи відправляється запит на видалення третім особам, яким передавались дані?

321 – Чи ознайомлений з правилами відкликання/видалення даних?

322 – Чи давалася згода на выдкликання даних?

323 – Чи має користувач можливість запросити видалення власних ПД?

331 – Чи можна експортувати дані з подальшим їх видаленням?

332 – Чи можна ознайомитися з правилами видалення даних?

333 – Чи є можливість подати запит на видалення персональних даних?

341 – Чи перевіряються запити на видалення даних?

342 – Чи є вимоги в часі по видаленню даних?

343 – Чи видаляються дані за закінченням терміну зберігання даних?

351 – Чи є доступ до сервера у сторонніх осіб?

352 – Чи прописана політика видалення даних?

353 – Чи проводяться пен-тести?

361 – Чи існує термін «життя» паролів?

362 – Чи прописан час зберігання тих чи інших даних?

363 – Чи можливо видалити пароль, у випадку його втрати?

371 – Чи можна запросити видалення всіх даних на ресурсі без пояснення причини?

372 – Чи прописані правила і термін видалення даних?

373 – Чи видаляються «непотрібні дані» (наприклад, які збирались для певних акційних пропозицій)?

381 – Чи існує повноцінна модель загроз для веб-ресурса?

382 – Чи прописаний набір експлоітів, зосереджених на безпеці даних?

383 – Чи доповнюється модель можливих загроз із появою нових серверів БД?

391 – Чи виконуються правила безпечного зберігання даних?

392 – Чи прописан ціль та термін зберігання даних користувачів?

393 – Чи видаляються дані за закінченням терміну дії?

3Х1 – Відмова запиті на видалення даних неможлива?

3Х2 – Чи вчасно видаляються дані користувачів, як вказано в політиці конфеденційності?

3Х3 – Чи відбувається регулярних перегляд запитів на видалення?

Питання блоку вимоги «Профілактика ризиків та комплексна перевірка»

411 – Чи проводиться регулярний аудит безпеки ИС?

412 – Адміністратор ознайомлений з правилами безпечного зберігання даних?

413 – Чи відбувається перевірка цілістності та конфеденційності зберігання даних?

421 – Чи прийняв користувач умови користування веб-ресурсом?

422 – Чи ознайомився з політикою безпеки на cookies?

423 – Чи оновлюється пароль з закінченням терміну дії?

431 – Політика конфеденційності знаходиться на видимому місці і доступна в один клік?

432 – Чи є можливість обрати, які саме cookies використовувати?

433 – Чи можливо видалити профіль і всю особисту інформацію?

441 – Чи мають треті особи доступ до оновлення даних?

442 – Чи прописані правила безппечного оновлення даних?

443 – Чи проводиться регулярний перегляд запитів на оновлення даних?

451 – Чи проводилось тестування на проникнення, згідно моделі загроз?

452 – Чи прописані вимоги щодо безпеки сервера?

453 – Чи безпечний сервер, на якому знаходиться веб-ресурс?

461 – Умови використання чіткі і зрозумілі?

462 – Чи використовується багатофакторна аутентифікація?

463 – Чи присутня капча?

471 – Чи є доступ до всіх даних користувачів у незареєстрованих юзерів?

472 – Чи приховуються контактні дані користувачів(якщо є) для неможливості використання ботами та парсерами?

473 – Політика конфеденційность знаходиться на видимому місці?

481 – Чи проводились тестування на проникнення?

482 – Набір експлоітів перевіряє всі можливі загрози?

483 – Чи доповнюється модель можливих загроз з появою нових серверів?

491 – Чи були випадки витоку даних користувачів?

492 – Чи створена модель порушника і всіх можливих загроз для веб-ресурса?

493 – Паролі зберігаються в хешованому вигляді?

4X1 – Чи має адміністратор доступ до паролів користувачів?

4X2 – Зберігання ПД відбувається так, як описано в угоді користувача?

4X3 – Чи є можливість змінити дані користувача без його відома?

Питання блоку вимоги «Повідомлення про витік даних»

511 – Адміністратор ознайомлений з правилами повідомлення про витік даних?

512 – Чи зазначений термін, в який має повідомлятися про витік?

513 – Чи повідомляється про випадки витоку/псування ПД користувачів?

521 – Чи ознайомлений з правилами витоку/псування ПД?

522 – Чи дана згода на політику конфеденційності?

523 – Чи повідомляється про випадки витоку/псування персональних даних?

531 – Чи є можливість запросити повідомлення про цілесність даних?

532– Чи прописано в угоді користувача правила повідомлення про витік?

533 – Чи відбувається перевірка правильності даних?

541 – Чи мають треті особи доступ до оновлення даних?

542 – Чи прописані правила повідомлення про виток даних?

543 – Чи проводиться регулярний перегляд запитів на оновлення даних?

551 – Чи проводилось тестування на проникнення, згідно моделі загроз?

552 – Чи прописані вимоги щодо безпеки сервера?

553 – Чи використовується ліцензований антивірус?

561 – Чи використовується «капча» для підтвердження того, що це людина?

562 – Чи прописан час зберігання тих чи інших даних?

563 – Чи можливо видалити пароль, у випадку його втрати?

571 – Чи є можливість не надавати ПД з поясненням, які функції веб-ресурса будуть недоступні?

572 – Чи є можливість обрати, які файли cookies може використовувати ресурс?

573 – Політика конфеденційность торкається витоку даних?

581 – Чи проводились тестування на проникнення?

582 – Набір експлоітів перевіряє всі можливі загрози?

583 – Чи доповнюється модель можливих загроз із появою нових серверів БД?

591 – Чи повідомляється користувачу про витік його даних?

592 - Чи повідомляється наглядовий орган про витік даних протягом 72 годин?

593 – Чи видаляються дані за закінченням терміну дії?

5X1 – Оновлення даних проводять лише з робочої машини?

5X2 – Оновлення виконує лише уповноважена особа (Адміністратор БД)?

5X3 – Чи є можливість змінити дані користувача без його відома?

ДОДАТОК Б

Програмний код матриці

Main.java

```
import java.util.Scanner;
public class Diplom {
    private final static Scanner scanner = new Scanner(System.in);
    public static void main(String[] args) {
        double q = 0;
        int iSize = 5, jSize = 10, kSize = 3;
        int n = iSize * jSize * kSize;
        int index = 0;
        Matrix matrix = new Matrix(iSize, jSize, kSize);
        for(; index < n; index++) {
            System.out.print(matrix.getElements()[index].getCoordinates()          +
"\nВВЕДІТЬ ЗНАЧЕННЯ: ");
            int value = scanner.nextInt();
            while(value < 1 || value > 5) {
                System.out.println("ЗНАЧЕННЯ ПОВИННО БУТИ ВІД 1 ДО 5!
ВВЕДІТЬ ЗНАЧЕННЯ ЩЕ РАЗ");
                value = scanner.nextInt();
            }
            matrix.insertValues(index, value);
        }
        // w = weight
        // b = value
        index = 0;
        for(double value, weight; index < n; index++) {
```

```
            Element element = matrix.getElements()[index];
            value = element.getValue();
            weight = element.getWeight();
            q += value*weight;
        }
        for (Element element: matrix.getElements()) {
            System.out.println(element);
        }
        System.out.printf("ВІДПОВІДНІСТЬ ВЕБ-РЕСУРСА ВИМОГАМ
GDPR: %f%n", q/n);
    }
}
```

Element.java

```
public class Element {
    final double B[] = { 0, 0.2, 0.2, 0.2, 0.2, 0.2};
    final double O[] = { 0, 0.04, 0.08, 0.1, 0.2, 0.06, 0.05, 0.07, 0.05, 0.1, 0.25};
    final double E[] = { 0, 0.2, 0.5, 0.3};
    private int i;
    private int j;
    private int k;
    private double value;
    private double weight;

    public void setI(int i){
        this.i = i;
    }
     public void setJ(int j){
        this.j = j;
    }
```

```
 public void setK(int k){
    this.k = k;
}
    public void setValue(double value){
    this.value = value;
    this.calculate();
}

public void setWeight(double weight){
    this.weight = weight;
}
  public int getI(){
    return i;
}
  public int getJ(){
    return j;
}
    public int getK(){
    return k;
}
    public double getValue(){
    return value;
}
    public double getWeight(){
    return weight;
}
    private void calculate(){
    weight = B[i] * O[j] * E[k] * value;
}
@Override
```

```
    public String toString() {
        return "КООРДИНАТА В МАТРИЦІ: i = " + i + ", j = " + j + ", k = " + k
+ "\nЗНАЧЕННЯ: " + value;
    }
}
```

Matrix.java

```
public class Matrix {
    private int iSize;
    private int jSize;
    private int kSize;
    private Element[] elements;

    public Matrix(int iSize, int jSize, int kSize){
        this.iSize = iSize;
        this.jSize = jSize;
        this.kSize = kSize;
        this.elements = new Element[iSize * jSize * kSize];
        this.makeCoordinates();
    }
    public void insertValues(int index, int value){
        elements[index].setValue(value);
    }
    public void makeCoordinates(){
        int index = 0;
        for(int i = 1; i <= iSize; i++){
            for(int j = 1; j <= jSize; j++){
                for(int k = 1; k <= kSize; k++){
```

```
                elements[index] = new Element();
                elements[index].setI(i);
                elements[index].setJ(j);
                elements[index].setK(k);
                index++;
            }
        }
    }
}
    public void setISize(int iSize){
    this.iSize = iSize;
}
    public void setJSize(int jSize){
    this.jSize = jSize;
}
  public void setKSize(int kSize){
    this.kSize = kSize;
}
    public void setElements(Element[] elements){
    this.elements = elements;
}
    public int getISize(){
    return iSize;
}
   public int getJSize(){
    return jSize;
}

public int getKSize(){
    return kSize;
```

```
        }
            public Element[] getElements(){
            return this.elements;
        }
}
```

На рисунку Б.1 зображено приклад використання програми і процес оцінки відповідності веб-ресурсу згідно питанням із додатку А.

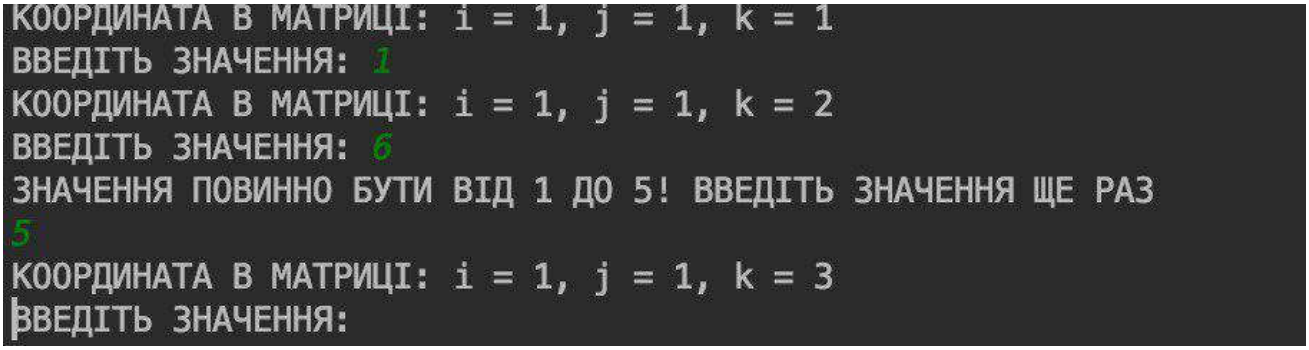

Рисунок Б.1 – приклад використання програми оцінки відповідності згідно опитувального листа

Кінцевим результатом є загальна оцінка відповідності веб-ресурса вимогам GDPR в шкалі від 0 до 1, що еквівалентна 100%.