

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ

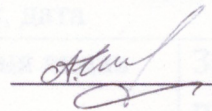
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології захисту персональних даних (на прикладі
благодійного фонду БФ "Відважні")»

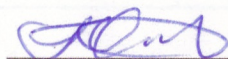
Виконала: студентка 2-го курсу групи ЗКбм-22-1
спеціальності 125 «Кібербезпека»

 Добровінська М.Г.

Керівник: доцент кафедри комп'ютерної інженерії
та кібербезпеки, кандидат технічних наук

 Шелуха О.О.

Рецензент: доцент кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

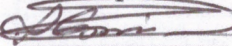
 Головня О.С.

Житомир – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Єфіменко А. А.

«13» 10 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студентки Добровінської Марії Геннадіївни

Тема роботи: **Методи та технології захисту персональних даних (на прикладі благодійного фонду БФ "Відважні")**

Затверджена Наказом університету від «13» жовтня 2023 р. №573/с

Термін здачі студентом закінченої роботи «25» грудня 2023 р.

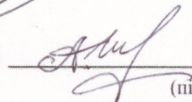
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Законодавство у сфері захисту персональних даних
2. Існуюча система захисту та обробки персональних даних організації
3. Програмне забезпечення для практичної реалізації

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються:

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

Студентка 

Керівник 

(підпис)

Календарний план (зміст)

№ з/п	Постановка завдання	Термін виконання етапів роботи	Відмітка про виконання
1.	Розробка вимог до проекту підсистеми захисту персональних даних	01.11.2023 – 03.11.2023	Виконано
2.	Аналіз методів та технологій захисту персональних даних клієнтів	04.11.2023 – 06.11.2023	Виконано
3.	Дослідження механізмів захисту персональних даних	10.11.2023 – 13.11.2023	Виконано
4.	Розробка програмного забезпечення	15.11.2023 – 17.11.2023	Виконано
5.	Тестування роботи розробленого програмного забезпечення	18.11.2023 – 23.11.2023	Виконано
6.	Аналіз результатів	24.11.2023 – 1.12.2023	Виконано
7.	Написання пояснювальної записки	3.12.2023 – 4.12.2023	Виконано
8.	Підготовка презентації та виступу	5.12.2023 – 9.12.2023	Виконано
9.	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	10.12.2023 – 12.12.2023	Виконано
10.	Захист	25.12.2023	Виконано

Студентка _____ Марія Добровінська

(підпис)

Керівник _____ Олексій Шелуха

(підпис)

ЗМІСТ

ВСТУП.....	
РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ БЛАГОДІЙНОЇ ОРАГНІЗАЦІЇ	
1.1. ВИДИ СУЧАСНИХ ДЖЕРЕЛ ТА МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ	
.....	
1.2. АНАЛІЗ НАЯВНИХ ТЕХНОЛОГІЙ ЗАХИСТУ ПЕРСОНАЛЬНИЙ ДАНИХ В БО «БФ «ВІДВАЖНІ»	
Висновки до 1-го розділу.....	
РОЗДІЛ 2. РОЗРОБКА ТЕХНІЧНИХ ВИМОГ ДО ДОДАТКА ДЛЯ РОБОТИ З ОСОБИСТИМИ ДАНИМИ БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ «БЛАГОДІЙНИЙ ФОНД «ВІДВАЖНІ»	
2.1. ОГЛЯД МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ТА ЇХ СПЕЦИФІКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ БЛАГОДІЙНИХ ОРГАНІЗАЦІЙ	
2.2. РОЗРОБКА ТЕХНІЧНИХ ВИМОГ ДО МАЙБУТНЬОГО ДОДАТКУ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ БФ «ВІДВАЖНІ».....	
2.3. РОЗРОБКА ПОШАГОВОГО АЛГОРИТМУ СТВОРЕННЯ ДОДАТКУ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.....	
Висновки до 2-го розділу.....	
РОЗДІЛ 3. ПЕРЕВІРКА ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОГО АЛГОРИТМУ.....	
3.1. АНАЛІЗ ЕФЕКТИВНОСТІ ТА ОПТИМІЗАЦІЇ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ОСНОВІ ЗАПРОПОНОВАНОГО АЛГОРИТМУ.....	

Висновки до 3-го розділу.....	
ВИСНОВКИ І ПРОПОЗИЦІЇ.....	
СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ.....	

ВСТУП

Інформація у ХХІ столітті виступає найбільш цінним ресурсом з усіх наявних. Використовуючись в економіці, політиці, військовій сфері, вона є важливим чинником для прийняття стратегічних та тактичних рішень. Отже, дане дослідження є актуальним, адже порушує насущну проблему добування та агрегації різноцільової інформації законним шляхом. У сучасному суспільстві неможливо обійтися без соціальних мереж і в сучасному світі переважають інтернет -технології. В даний час кожна людина, пов'язана з комп'ютером, зареєстрована хоча б в одній соціальній мережі. Соціальні мережі притягують людей, так як в сучасному світі всі люди спілкуються, обмінюються інформацією, знайомляться. Аналіз методів захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії, показав що неможливо віддати перевагу якомусь одному методу захисту персональної інформації.

Захист від загроз, які не залежать від атак, регулюється інструкціями, розробленими та затвердженими уповноваженими службами розпорядника персональних даних, з урахуванням специфічних умов функціонування інформаційної системи, атакож чинних нормативних документів. Захист від загроз, які можуть бути реалізовані внаслідок атаки, повинен забезпечуватися за допомогою захисних заходів і засобів, які використовуються інформаційною системою і призначені переважно для протидії атакам. Атака соціальної інженерії має спільну структуру. Вони відбуваються в один або кілька кроків.

Згідно з українським законодавством не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. А отже, загрози персональним даним можна описати наступним чином -це загрози несанкціонованого зберігання, використання та поширення конфіденційних даних.

Сучасні підприємства створюють кіберзахист, орієнтуючись насамперед на технічні вектори атак. Такі системи можуть мати високий рівень зрілості і здаватися надійними, але при цьому залишатися уразливими для однієї з найнебезпечніших загроз - соціальної інженерії, заснованої на маніпуляціях людською свідомістю.

Метою роботи є поглиблення теоретичних знань у сфері захисту персональних даних при роботі благодійної організації та використання здобутих знань під час реалізації діяльності БО «БФ «ВІДВАЖНІ» для створення ефективної, а головне захищеної інформаційної системи, яка сприятиме покращенню інформаційно-комунікаційної системи Благодійної організації.

Об'єктом дослідження виступають персональні дані працівників, волонтерів, підопічних та тих, хто звертається до Фонду за допомогою чи підтримкою.

Предметом дослідження є система персональних даних, яка вже наявна в БО «БФ «ВІДВАЖНІ». Для досягнення зазначеної мети необхідним є вирішення наступних взаємозалежних науково-технічних задач:

- Розробка вимог до проєкту підсистеми захисту персональних даних благодійної організації
- Аналіз технологій передачі та збереження даних клієнтів
- Опис та алгоритми роботи обраної інфраструктури та хмарного сервісу
- Дослідження механізмів захисту персональних даних
- Створення покрокового алгоритму розробки додатку для захисту персональних даних
- Розробка скриптів для початкового налаштування системи
- Вимірювання допустимої ефективності використання застосунку та його вплив на швидкість виконання задач для оптимізації роботи організації.
- Аналіз результатів.

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ БЛАГОДІЙНОЇ ОРАГНІЗАЦІЇ.

1.1. ВИДИ СУЧАСНИХ ДЖЕРЕЛ ТА МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Усі методи захисту персональних даних цілеспрямовано впливають на захист інформації, але захист в повному обсязі неможливо забезпечити тільки одним методом.

З повномасштабним вторгненням в Україні значно виріс попит та потреба у волонтерській та благодійній діяльності, що в свою чергу вплинуло на значний зріст зареєстрованих організацій, діяльність яких спрямована саме на покриття соціальних потреб. Так як, в Україні всі реєстри станом на повномасштабне вторгнення, за причин безпеки закриті, перевірити або запросити данні – майже нереально, кожна із організацій почала створювати свої системи, методи та можливі варіанти захисту персональних даних. Спираючись на аналіз методів захисту персональних даних, запропоновано удосконалений метод захисту персональних даних від атак за допомогою алгоритмів ІТ-сфери та сфери кібербезпеки, створивши алгоритми майбутніх застосунків.

Соціальна інженерія –це такий нетехнічний тип стратегії кібератак, який базується на взаємодії між людьми та маніпуляціях таким чином, щоб людина порушила стандартні правила кібербезпеки.

Проте соціальна інженерія вимагає від зловмисника гарної підготовки, що зазвичай має на меті збір інформації про жертву, аби точно знати, як саме можна отримати бажану інформацію.

Закон України “Про інформацію” [1] окреслює конфіденційну інформацію як інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. У сучасному світі найуразливішою ланкою серед усіх кібератак залишається людина. Персональні дані можуть бути як

конфіденційною інформацією, так і відкритою. Пункт 2 статті 11 Закону України “Про інформацію” [1] встановлює, що конфіденційними є зокрема дані про національність, освіту, сімейний стан, релігійні переконання, стан здоров’я, місце проживання і/або реєстрації, дата і місце народження. Закон України “Про захист персональних даних” [2] визначає персональні дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Це найуживаніше визначення даного поняття -і воно є найбільш узагальненим. Перелік відомостей, які належать до персональних даних, змінюється від однієї держави до іншої. Наприклад, інформація про IP-адресу в країнах Європейського Союзу належить до персональних даних, а у Сполучених Штатах Америки ні, проте відноситься до інформації, що пов’язана з персональними даними.

Сучасні підприємства створюють кіберзахист, орієнтуючись насамперед на технічні вектори атак. Такі системи можуть мати високий рівень зрілості і здаватися надійними, але при цьому залишатися уразливими для однієї з найнебезпечніших загроз -соціальної інженерії, заснованої на маніпуляціях людською свідомістю. За статистикою, сьогодні соцінженерія так чи інакше застосовується в 97% націлених атак, при цьому технічні вектори часом взагалі не використовуються або використовуються мінімально. На перші місця серед загроз інформаційної безпеки ставляться методи соціальної інженерії, а ряд вчених стверджує, що якщо соціальна інженерія візьме на озброєння технології машинного навчання і штучного інтелекту, то людство отримає загрозу, яку можна порівняти з глобальним потеплінням і ядерною зброєю. У просунутих варіантах соціальна інженерія -це витончена галузева політика «професійних» команд шахраїв і технічних фахівців різних профілів. Тому питання вивчення методів впливу на безпеку персональної інформації –соціальної інженерії є дуже актуальним.

Захист персональних даних фізичних осіб в Україні наразі регулюється Законом України «Про захист персональних даних» від 01.06.2010 № 2297-VI (далі – Закон № 2297).

Згідно з Законом № 2297 обробкою персональних даних є будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

Закон № 2297 регулює такі основні питання обробки персональних даних:

- вимоги до обробки персональних даних;
- права суб'єктів персональних даних;
- підстави для обробки персональних даних;
- порядок здійснення основних процесів обробки персональних даних (збирання, використання, накопичення та зберігання, поширення, видалення);
- порядок обробки персональних даних, обробка яких становить особливий ризик для прав і свобод суб'єктів персональних даних тощо.

Проте, в епоху бурхливого розвитку цифрових технологій діюче законодавство про захист персональних даних все більше й більше застаріває. Воно не забезпечує належного захисту суб'єктів персональних даних при обробці персональних даних з використанням інформаційних технологій та не містить достатніх гарантій прав суб'єктів даних у разі витоку персональних даних, що містяться у базах даних володільця персональних даних.

У зв'язку зі змінами, які відбулися у економіці та соціальному житті, українське законодавство потребує повного оновлення правового регулювання процесів обробки персональних даних.

За численними повідомленнями в засобах масової інформації громадяни України постійно піддаються хакерським атакам з боку ворожих кіберзловмисників. Мають місце надсилання електронних листів, повідомлень у месенджерах від начебто державних органів, банків, служби безпеки тощо з рекомендаціями перейти за вказаними у листах/повідомленнях посиланнями. Після завантаження вкладеного файлу зловмисники мають змогу отримати

доступ до персональних даних, що містяться на 8 електронному пристрої користувача (контактів телефонної книги, файлів персонального комп'ютера тощо). Щоб не стати жертвою кіберзловмисників необхідно уважно ставитись до електронних листів від незнайомих адресатів, повідомлень у месенджерах (Viber, Telegram, WhatsApp) з невідомих номерів телефону, а також повідомлень в соціальних мережах (Facebook) від незнайомих користувачів.

У разі їх надходження не відкривати підозрілі посилання та не завантажувати вкладені файли. Відкриття таких посилань або файлів може спричинити завантаження шкідливого програмного забезпечення на пристрій і отримання доступу до персональних даних. Необхідно користуватись перевіреними джерелами інформації – наразі це офіційні сторінки державних органів України, які оприлюднюють інформацію та посилання на сервіси щодо знаходження прихистку, розшуку зниклих, отримання допомоги, проведення евакуації тощо.

Щоб вберегти свої персональні дані рекомендується зробити резервні копії документів, фото, телефонної книги, які необхідно зберігати у надійному місці. Також доцільно виписати номери телефонів найближчих членів родини. Це допоможе не втратити зв'язок з найдорожчими навіть якщо буде втрачено контроль над пристроєм.

Приймаючи до уваги швидкий технологічний розвиток та глобалізацію економіки на рівні Європейського Союзу був затверджений Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб при обробці персональних даних та про вільний рух таких даних (далі — Загальний регламент про захист даних), який скасував діючу раніше Директиву 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. На відміну від Директиви 95/46/ЄС норми Загального регламенту про захист даних є нормами прямої дії, а, отже, вони не потребують імплементації у внутрішнє законодавство країн

Європейського Союзу та застосовуються у всіх країнах Європейського Союзу з моменту набуття Регламентом чинності, тобто з 28 травня 2018 року.

Згідно зі статтею 15 Угоди про асоціацію України та Європейського Союзу Україна та Європейський Союз домовилися співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи.

Для України це означає імплементацію європейських стандартів захисту персональних даних в українське законодавство.

При обробці персональних даних необхідно буде дотримуватися таких принципів обробки даних як:

- Законність, добросовісність та прозорість;
- Обмеження мети;
- Мінімізація персональних даних;
- Точність персональних даних;
- Обмеження зберігання;
- Цілісність і конфіденційність;
- Персональні дані зможуть оброблятися лише з підстав, що передбачені законодавством.

Якщо обробка даних буде здійснюватися на підставі згоди суб'єкта даних, то така згода повинна бути:

- вільно вираженою – це означає право вільного вибору для суб'єкта даних та відсутність тиску;
- спеціальною — тобто наданою на обробку даних з певною метою;
- здійсненою у формі активних дій – надання згоди у формі мовчазної згоди, шляхом конклюдентних дій не буде законним;
- інформованою – тобто суб'єкту даних слід буде надати інформацію про особу, яка обробляє дані, та процеси обробки до моменту отримання згоди;

- недвозначною – тобто ясно виражена вказівка щодо бажань суб'єкта даних на обробку його персональних даних.

Органи державної влади, органи місцевого самоврядування, підприємства, установи і організації усіх форм власності, фізичні особи – підприємці, фізичні особи, що провадять незалежну професійну діяльність, які обробляють персональні дані, зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних. Варто зауважити, що використання персональних даних здійснюється у разі створення умов для захисту цих даних. Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом. Такі обов'язки визначені у статтях 10, 24 Закону України «Про захист персональних даних», які стосуються питань використання персональних даних та забезпечення захисту персональних даних.

Мета обробки персональних даних – це важливий пункт при взаємодії з чутливими верствами населення, зі співробітниками/волонтерами/донорами, які хочуть допомагати і бути захищеними від третіх осіб та це вимагає від благодійних організацій приділення особливої уваги та відповідності законодавству.

1.2. АНАЛІЗ НАЯВНИХ ТЕХНОЛОГІЙ ЗАХИСТУ ПЕРСОНАЛЬНИЙ ДАНИХ В БО «БФ «ВІДВАЖНІ»

БФ «ВІДВАЖНІ» мають основні два напрямки діяльності: мами з дітьми та люди літнього віку. З перших днів війни волонтери Фонду підтримують психологічно та в наданні гуманітарної допомоги, зазначені вище, соціальні групи. За 1,5 роки було опрацьовано більше 15000 запитів та привезено близько 150 тон гуманітарної допомоги. З перших днів повномасштабного вторгнення росії на територію України, місто Коростень стало транзитним між Сходом та Заходом. Відповідно запит на забезпечення людей допомогою зростає з кожним днем, а отже і бази персональних даних також. Станом на зараз налічується постійних 100 сімей, які є підопічними Фонду та близько 170 людей літнього віку, яким на постійні основі, один раз на місяць, надається допомога. Відповідно пропозиція щодо збереження персональних даних полягає в наступному.

Є два засновники: один відповідає за зовнішні фактори (інвестори, гроші, гранти, партнери), а інший — за внутрішні (волонтери, налагодження роботи в команді, розподіл ролей та відповідальності).

У роботі Фонду є два напрямки:

- Проєктна діяльність;
- Гуманітарна допомога;

Проєктна діяльність - це реалізація різноманітних заходів: отримання гранту та його використання для організації концерту для дітей, допомога організаціям у зборі коштів або підтримці таких зборів, чи проведення курсів з медіаграмотності для підлітків. Усі ці процеси завжди супроводжуються збором даних (дітей, батьків, згоди батьків на участь їхніх дітей у таких курсах/заходах, збору зворотного зв'язку від дітей та батьків через форми, де вони також вносять свої контактні дані).

Гуманітарна допомога – є літні люди, яким Фонд допомагає їжею та спеціальною гігієною. За кожною парою волонтерів закріплений маршрут та

люди, яким потрібно протягом 5 днів щомісяця роздавати ці продукти чи гігієну, складати звіт на місці (кому видали чи кому передали, бо частіше всього родичі забирають) і по приїзду скласти звіт, скільки всього роздали і скільки залишилося/не взяли.

Персональні дані є важливим інструментом у роботі БФ «ВІДВАЖНІ», тому їх коректне збереження – це, в першу чергу, безпека людей, які працюють та людей для яких створюються умови та проекти. У період повномасштабного вторгнення вже важче і важче зберігати таку інформацію, адже звичайні гугл-таблиці не дають ніякої гарантії, що інформація з них залишиться конфіденційною та не буде використана іншими особами. Станом на зараз Фонд не має ніякого програмного забезпечення чи системи, яка б могла збирати, систематизувати та берегти конфіденційно інформацію людей.

Загальновідомо, що обробка персональних даних має ґрунтуватись на меті та правових підставах. Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних.

Згідно із Законом України «Про правовий режим воєнного стану» воєнний стан передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності. Водночас відповідно до частини другої статті 19 Конституції України органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. У такому випадку підставами для обробки (збирання, реєстрації, накопичення, зберігання, адаптування,

зміни, поновлення, використання, поширення, знеособлення, знищення тощо) персональних даних відповідними державними органами та органами місцевого самоврядування є пункти 2 та 5 частини першої статті 11 Закону України «Про захист персональних даних», а саме: • дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень; • необхідність виконання обов'язку володільця персональних даних, який передбачений законом.

Володільці, розпорядники персональних даних самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних та інформаційної безпеки. Організаційні заходи охоплюють:

- визначення порядку доступу до персональних даних працівників/володільця/розпорядника;
- визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;
- розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- регулярне навчання співробітників, які працюють з персональними даними.

Працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків.

Відповідно до ст. 1 ЗУ “Про обробку персональних даних”, персональні дані — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (далі – ПД).

Відповідно до ст. 3 ЗУ “Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”

ідентифікувати — здійснювати комплекс заходів, що дає змогу виконувати пошук за принципом “один до багатьох”, зіставляючи дані (параметри) особи, у тому числі біометричні, з інформацією Реєстру;

ідентифікація особи — встановлення особи шляхом порівняння наданих даних (параметрів), у тому числі біометричних, з наявною інформацією про особу в реєстрах, картотеках, базах даних тощо;

Таким чином, за наявності інформації, яка дає змогу безпомилково виділити особу з-поміж інших осіб, може тлумачитись, як “ідентифікована”. Отже, в практичному сенсі це може виглядати так: якщо є ім’я, прізвище, по батькові та відповідні реквізити документів, що посвідчують особу, або, наприклад, реєстраційний номер облікової картки платника податку (далі – РНОКПП), то це є беззаперечним фактом того, що особа ідентифікована. Звісно, бувають випадки, за яких навіть за наявності меншої кількості інформації, цього достатньо, щоб ідентифікувати особу. Та це треба доводити стороні, яка оскаржує обробку персональних даних.

У багатьох благодійних організаціях надаються адресні благодійні допомоги, які зазвичай потребують в обробці ПІБ, паспортні дані/РНОКПП, телефон. Ці дані дають змогу ідентифікувати особу.

Персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

З метою забезпечення безпеки обробки персональних даних володільцями, розпорядниками вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних.

Отже, у разі здійснення обробки персональних даних необхідно створити належні умови для їх захисту.

За таких обставин, для обробки персональних даних отримувачів благодійної допомоги слід керуватись наступними підставами для обробки, які визначені ст. 11 ЗУ “Про обробку персональних даних”:

1. Згода суб’єкта персональних даних на обробку його персональних даних;

2. Укладення та виконання правочину, стороною якого є суб’єкт персональних даних або який укладено на користь суб’єкта персональних даних чи для здійснення заходів, що передують укладенню правочину, на вимогу суб’єкта персональних даних;

Щодо першої підстави Ст. 2 ЗУ «Про обробку персональних даних» наводиться поняття згоди суб’єкта персональних даних – це добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.

Ч. 2 статті 12 ЗУ “Про обробку персональних даних” вимагає повідомлення суб’єкта персональних даних про:

А) Володільця персональних даних;

Б) Склад та зміст зібраних персональних даних;

В) Свої права, визначені Законом;

Г) Мету збору персональних даних та осіб, яким передаються його персональні дані.

Виходячи з вищенаведеного, в згоді на обробку персональних даних повинна бути інформація, яка вимагається у пунктах А-Г. Окрім того, на володільця персональних даних покладається обов’язок довести, що згода є і суб’єкт персональних даних обізнаний з пунктами А-Г.

Крім того, передбачена у статті 7 Закону України «Про захист персональних даних» заборона на обробку персональних даних, про расове

або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних не застосовується, якщо обробка персональних даних, зокрема, стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом. 4 Таким чином, в умовах введеного в Україні воєнного стану захист персональних даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних, захист державних інформаційних ресурсів, ІТ-систем об'єктів критичної інфраструктури, державних реєстрів, які містять персональні дані є вкрай важливими. Обробка персональних даних має здійснюватися з урахуванням викладених вище положень законодавства України. Така обробка має бути пропорційною та здійснюватися для конкретних і законних цілей.

Працівники Фонду, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних обов'язків.

Висновки до 1-го розділу

Усі методи захисту персональних даних цілеспрямовано впливають на захист інформації, але захист в повному обсязі неможливо забезпечити тільки одним методом.

Персональні дані є важливим інструментом у роботі БФ «ВІДВАЖНІ», тому їх коректне збереження – це, в першу чергу, безпека людей, які працюють та людей для яких створюються умови та проекти.

Життєво важливих інтересів. Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим. Згода суб'єкта персональних даних – це добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційнокомунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки. Враховуючи викладене, згода на обробку персональних даних має відповідати таким вимогам: 7 ✓ добровільність – означає відсутність прямого або опосередкованого примусу при її наданні; ✓ поінформованість – означає, що перед наданням згоди суб'єкт повинен отримати достовірну інформацію про те, ким, з якою метою будуть оброблятися його персональні дані, кому будуть передаватися, які саме дані, а також про права, визначені Законом; ✓ форма надання згоди може бути будь-якою – означає, що умови згоди на обробку персональних даних можуть бути викладені у формі єдиного письмового документа, викладеного доступною для суб'єкта персональних даних мовою, що підписується ним особисто або його

законним представником, у електронній формі проставивши відмітку про надання згоди, або ж навіть усно. Водночас надана згода не повинна викликати сумнівів в її однозначності і володілець повинен мати змогу підтвердити її наявність упродовж усього часу здійснення обробки персональних даних. Разом з тим необхідно враховувати пропорційність обсягу персональних даних суб'єкта. Оброблятися повинні лише ті дані, обробка яких необхідна для досягнення мети. Все залежить від критеріїв, за якими відбувається надання матеріальної чи іншої благодійної/гуманітарної допомоги (категорії суб'єкта, стану здоров'я, матеріального забезпечення, сімейного статусу, кількості дітей тощо). Отже, якщо для надання адресної благодійної допомоги необхідно здійснювати обробку персональних даних, то варто відповідально підійти до питання оформлення правовідносин та забезпечити захист персональних даних.

РОЗДІЛ 2. РОЗРОБКА ТЕХНІЧНИХ ВИМОГ ДО ДОДАТКА ДЛЯ РОБОТИ З ОСОБИСТИМИ ДАННИМИ БЛАГОДІЙНОЇ ОРГАНІЗАЦІЇ «БЛАГОДІЙНИЙ ФОНД «ВІДВАЖНІ».

2.1. ОГЛЯД МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ТА ЇХ СПЕЦИФІКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ БЛАГОДІЙНИХ ОРГАНІЗАЦІЙ.

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

Дії можуть вчинятися під час обробки персональних даних:

- **Збирання:** суб'єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, мету збору персональних даних та осіб, яким передаються його персональні дані:
 - в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних;
 - в інших випадках протягом 30 робочих днів з дня збору персональних даних.
- **Накопичення персональних даних** - дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення цих даних до бази персональних даних.
- **Зберігання персональних даних** - дії щодо забезпечення їх цілісності та відповідного режиму доступу до них.
- **Поширення персональних даних** - дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних. Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.

Виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані. Персональні дані наразі - найцінніше, що є у віртуальному світі.

Перед тим, як завантажувати будь-який додаток, бажано дізнатись, хто розробники, як вони зберігають ваші дані і як використовують.

Нині на рівні держави також запускають багато цікавих ініціатив: E-health, ДІЯ та інші проекти. Приємно розуміти, що ми одні з небагатьох країн світу, хто запустив і продовжує запроваджувати такі послуги онлайн.

Гарна мета - покращення нашого життя та зменшення бюрократичних і корупційних складових. Проте треба розуміти, що саме питання кібербезпеки є ключовим для довіри громадян та використання онлайн сервісів. Якщо ваші дані просять надати державні органи, потрібно також цікавитись, якими є стандарти зберігання і де їх будуть тримати.

Коли держава запускає глобальні рішення, бажано публічно заявляти розробника, а також відповідального за кібербезпеку (зазвичай це окрема компанія).

В західних країнах розробники із задоволенням говорять про кіберзахист. У такий спосіб вони акцентують увагу на турботі про своїх користувачів. Надійний захист даних, безперечно, є конкурентною перевагою, тому що споживач на це вже звертає увагу.

У галузі захисту від сучасних кібератак одна із новітніх тенденцій - використання аналітичних систем кібербезпеки із застосуванням систем машинного навчання і штучного інтелекту на великих обсягах даних (Machine Learning-based Security Analytics using Big Data).

Ці системи дозволяють помічати відхилення у поведінці систем чи користувачів від норми і таким чином виявляти більшість небезпечних кібератак. Перспективним є застосування таких систем для завдань кібербезпеки у вигляді платформ UEBA (User Entity and Behavior Analytics).

Тривіальний приклад: якщо користувач зайшов у систему в незвичний час, почав передавати незвичний обсяг інформації в інтернет, то має місце "аномальна поведінка" даного користувача, і вона автоматично розпізнається платформою кібербезпеки EBUA.

Звісно, ідеальних технічних рішень не існує, але застосування найбільш сучасних когнітивних технологій кіберзахисту безперечно "піднімає планку вимог" для кіберзлочинців.

2.2. РОЗРОБКА ТЕХНІЧНИХ ВИМОГ ДО МАЙБУТНЬОГО ДОДАТКУ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ БФ «ВІДВАЖНІ».

Успішна розробка потребує детального вивчення та чіткого планування. Так, після всіх досліджень, мозкових штурмів і ретельного аналізу всі деталі про майбутній програмний продукт викладаються в технічного завдання для мобільного додатка. Цей документ - запорука точності попадання на всі очікування, закриття всіх потреб і взагалі успіху в реалізації проекту. Без нього не буває розробки, адже команда просто не знатиме, що робити.

Вимоги для початку проекту бувають двох типів –

- 1) Професійні
- 2) Технічні

З першого пункту ми маємо вилучити необхідних спеціалістів для початку розробки проекту.

В нашому випадку нам потрібні:

- 1) Архітектор
- 2) UI/UX Дизайнер
- 3) Графічний дизайнер
- 4) Front-end розробник
- 5) Back-end розробник
- 6) SQL розробник
- 7) Devops

Вище перелічені базові спеціалісти для проекту будь якої складності. Кожен з перелічених професіоналів має навички в сфері які знадобляться нам, звичайно варіація спеціалістів може бути декілька різною і варіативною, це вже залежить саме від технічного стеку та вимог на проєкті.

Технічний стек:

- 1) FIGMA
- 2) PhotoShop
- 3) HTML

- 4) CSS
- 5) SASS
- 6) JavaScript
- 7) jQuery
- 8) Composer
- 9) PHP
- 10) OPanel
- 11) MySQL

Ще існують загальні вимоги сучасних стандартів, вони означають:

- 1) Кроссбраузерність
- 2) Адаптивність
- 3) Можливість підтримки
- 4) Універсальність

Опис покрокової розробки проекту

1 – Архітектура

Першим етапом і саме фундаментом проекту є Архітектура, саме вона відповідає за майбутню логіку додатку та складність розробки. Особливість цього етапу – складність в створенні скелету через велику кількість даних з якими доведеться працювати та грамотність їх передачі та обробки.

Також до складності цього процесу можна віднести відповідальність, стати архітектором без глибоких знань сфери та багатьох років роботи в ній – неможливо.

2 – Дизайн

Цей момент схожий за реалізацією але різний по складності і головній меті, з архітектурою.

На цьому етапі UX/UI та графічний дизайнер створюють макет застосунку та його анімації

Детальніше до цього пункту ми перейдемо пізніше, але, зокрема, чогось цікавого в цьому процесі, нажаль, нема. До складнощів можна віднести лише натхнення дизайнера та який в нього настрій, тож гайда далі.

З – Нарешті ми дійшли до розробки Front-end частини нашого додатку

Це та ступінь коли розробник переписує макет дизайну за допомогою HTML та CSS

HTML - Hypertext Markup Language. Він допомагає створити саме розмітку нашої сторінки за допомогою тегів та підключень різних файлів, а також присвоїти стилі які ми пишемо за допомогою CSS/SCSS

```
<div class="tabs flex-tabs">
  <label for="tab-one" id="tab-one-label" class="tab">DESCRIPTION</label>
  <label for="tab-two" id="tab-two-label" class="tab">PRODUCT DETAILS</label>
  <div id="tab-one-panel" class="panel active">
    <?php the_content( $more_link_text, $strip_teaser ); ?>
  </div>
  <div id="tab-two-panel" class="panel">
    <ul class="product-details">
      <li>
        <span class="product-detail-info">Brand</span>
        <span class="product-detail-info"><?php the_field('brand_fabric'); ?></span>
      </li>
      <li>
        <span class="product-detail-info">Country</span>
        <span class="product-detail-info"><?php the_field('country'); ?></span>
      </li>
    </ul>
  </div>
</div>
```

Приклад коду HTML

CSS – Cascading Styles Sheets. Формальна мова написання стилів візуалізації та вигляду нашої сторінки. За допомогою CSS ми створюємо анімації, регулюємо порядок наших елементів, їх форму, колір та усі інші візуальні характеристики

```
.burger.active .third {
  transform: rotate(-45deg) translateY(50%);
  bottom: 50%;
}

.container {
  width: 100%;
}

.header {
  display: flex;
  height: 100px;
  background: #FFFFFF;
  width: 100%;
  max-width: 1920px;
  margin: 0 auto;
  justify-content: center;
  position: relative;
}
```

Для того щоб вказати пошуковим системам, які індексують веб-сторінки, що їм не слід індексувати конкретну сторінку або весь сайт, використовується файл robots.txt та мета-теги HTML. Вам необхідно внести відповідні зміни на вашому сайті. Ось як це можна зробити:

1. Використання файлу robots.txt:

Створіть файл robots.txt на кореновому рівні вашого сайту та включіть необхідні директиви.

Наприклад, якщо ви хочете заборонити індексацію всього сайту, вміст файлу robots.txt може виглядати так:

User-agent: *

Disallow: /

Це створить правило для всіх пошукових ботів (User-agent: *) не індексувати жодну сторінку на вашому сайті (Disallow: /).

2. Використання мета-тегів HTML:

Якщо вам потрібно заборонити індексацію окремої сторінки, вставте мета-тег в розділ <head> цієї сторінки.

```
<meta name="robots" content="noindex, nofollow">
```

Це вказує пошуковим системам не індексувати (noindex) та не відстежувати посилання з цієї сторінки (nofollow).

Оберіть метод, який вам більше підходить, або використовуйте обидва для більшої надійності. Після внесення змін, слід перевірити їх правильність за допомогою різних інструментів для аналізу файлу robots.txt та індексації сторінок пошуковими системами.

Для того щоб залишити на сайті повідомлення на випадок взлому і вказати контактну інформацію для повідомлення про виявлені вразливості, ви можете використовувати спеціальні сторінки та контактні форми. Ось кілька рекомендацій:

1. Створіть Сторінку "Зв'яжіться з Нами" або "Повідомте про Вразливості"

Створіть спеціальну сторінку на вашому сайті, на якій буде вказано, як зв'язатися з вашою командою в разі виявлення вразливостей або випадку взлому. Розмістіть на цій сторінці інформацію для зв'язку, таку як електронна пошта, номер телефону або інші зручні засоби.

2. Використовуйте Форму Зворотнього Зв'язку або Контактну Форму.

Розмістіть на своєму сайті контактну форму або спеціальну форму для повідомлення про вразливості. Забезпечте можливість анонімного повідомлення та надайте докладні інструкції щодо того, якою інформацією слід поділитися.

3. Використовуйте Файл robots.txt для Повідомлення про Власника.

Ви також можете внести зміни у файл robots.txt, де вказати шлях до спеціальної сторінки або контактної форми, яку слід використовувати для повідомлень про вразливості. Наприклад:

User-agent: *

Disallow: /path/to/vulnerability-page

4. Публікуйте Інформацію на Сторінці "Про Нас"

Розмістіть інформацію про те, як повідомити про вразливості або інцидент на сторінці "Про нас" чи "Контакти".

5. Зашифруйте З'єднання та Використовуйте SSL

Впевніться, що ваш сайт використовує SSL для зашифрованого з'єднання. Це забезпечить конфіденційність інформації, яку користувачі надсилають через форми зворотного зв'язку.

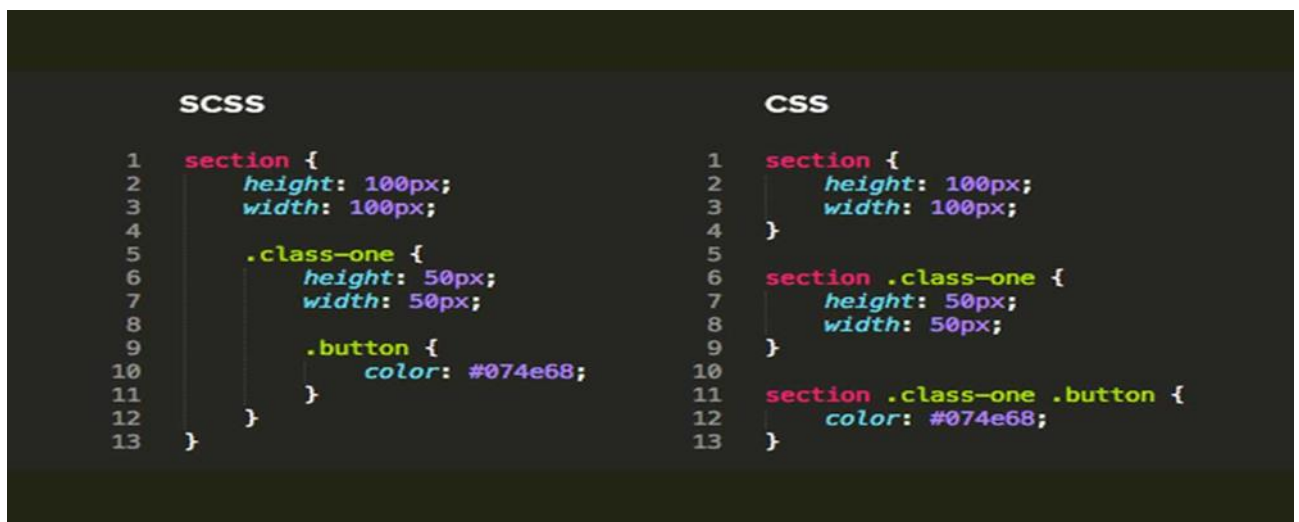
Не забувайте регулярно перевіряти ці контактні канали і вносити необхідні оновлення для забезпечення ефективної комунікації та відповіді на виявлені проблеми чи вразливості.

Приклад коду на CSS

В цей раз на нашому проєкті ми використовуємо SCSS – Препроцесор для CSS. Препроцесора використовуються саме для зменшення кількості коду, так як CSS зазвичай займає від 5000 ліній тексту.

Головними особливостями SCSS :

- Існування контексту який задекларований знаком Амперсанта “&”, цей знак зсилає нас до класу з яким ми працюємо в локальній області видимості;
- Наявність Міксинів – спеціальний стиль в якому ми записуємо CSS якості і відтворюємо їх за допомогою передачі аргументів в міксин, де ми його викликаємо;
- Наявність шаблонів – клас який не зав’язаний за чимось і зазвичай має глобальні параметри, колір бренду чи стилі для скролбару;
- Функцію – чисті функції які зазвичай написані для додавання стилів в залежності від інших факторів які має клас.



Відмінність написання коду між CSS – SCSS

Остання і найголовніша Front-end технологія про яку ми поговоримо - JavaScript(далі JS) – Мова скриптів сайту. Саме в JS ми прописуємо всіх

слухачів подій, які відбуваються при взаємодії з елементами нашого DOM дерева (деревоподібна структура архітектури нашої HTML сторінки)

```
const skipAddBtn = document.getElementById("skipAddButton")
skipAddBtn.addEventListener("onclick", e => {e.preventDefault()})
```

Приклад отримання кнопки з DOM та запобігання виконанню її стандартної поведінки

Саме за допомогою JS ми отримуємо данні про елемент і додаємо йому функціонал, саме за допомогою JS ми можемо говорити нашій програмі коли робити запити до Back-end скриптів і за яких умов. В нашому проєкті ми будемо використовувати jQuery – це величезна бібліотека функцій для JS, сама по собі вона не містить особливого функціоналу, а лише скорочує кількість коду.

```
jQuery(document).ready(function ($) {
  $('.btn-load-more').click(function (e) {
    e.preventDefault();
    const button = $(this),
      data = {
        'action': 'load_more',
        'query': load_more.posts,
        'page': load_more.current_page,
        'nonce': load_more.nonce
      };
    $.ajax({
      url: load_more.ajaxurl,
      data: data,
      type: 'POST',
      success: function (data) {
        if (data) {
```

Приклад коду на jQuery в якому ми асинхронно відправляємо дані методом POST

2.3. РОЗРОБКА ПОШАГОВОГО АЛГОРИТМУ СТВОРЕННЯ ДОДАТКУ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.

В сучасній веб розробці ніхто не створює окремі додатки для захисту персональних даних, а одразу прописують їх логіку при передачі даних. Найголовніша частина Back-end це саме створити логіку передачі даних між клієнтом-проектом-сервером і саме паралельно написанню цієї логіки прописуються ще і правила які допомагають захистити данні від хакерів та інших недобросовісних людей. Ми не будемо обговорювати тему протоколів так як це можна було б розтягнути ще на сотню сторінок, але згадаємо найпопулярніший, в наш час, з них – HTTPS. HTTPS – це протокол передачі даних, який шифрує данні при їх передачі, для розшифрування яких має унікальний ключ.

Методи забезпечення безпеки даних:

- Валідація даних з форм;
- Валідації SQL запитів;
- Забезпечення коду якісними перевірками при виконанні скриптів;
- Обмеження даних які може бачити вводити клієнт до мінімуму;
- Валідація від SVG ін'єкцій;
- Шифрування даних;
- Використовування регулярних виразів.

Усі вищезазначені пункти ми будемо використовувати в нашому додатку, на кожному ми не будемо зупинятися, але я поясню за найпрактичніші

1 – Дані які вписує користувач, в тому числі паролі і логіни, повинні перевірятися регулярними виразами та опрацьовуватися за допомогою попередньо задекларованої функції

```
function data_validation($data)
{
    $data = trim($data);
    $data = stripslashes($data);
    $data = htmlspecialchars($data);
    return $data;
}
```

Приклад функції опрацьовувача

В цю функцію ми передаємо аргументом строку з даними і спочатку обрізаємо пробіли в початку та кінці за допомогою **trim()**. За допомогою **stripslashes()** ми видаляємо екранування символів **htmlspecialchars()** перетворює спец символи в html сутності, наприклад, замінюють знак амперсанту в &. Ця функція забороняє клієнту робити ін'єкції які можуть потрапити через форму у запит до бази даних

```
$errors_list = [];
if ($_SERVER["REQUEST_METHOD"] == "POST") {
    if ($_POST["registration-nicename"] && $_POST["registration-nicename"] != "") {
        $registered_nicename = data_validation($_POST["registration-nicename"]);
    } else {
        $errors_list["nicename_err"] = "Username is required";
    }
    if ($_POST["registration-password"] && $_POST["registration-password"] != "") {
        $registered_password = data_validation($_POST["registration-password"]);
        if (strlen($registered_password) < 6) {
            $errors_list["password_err"] = "Password must be longer 6 characters";
        }
    } else {
        $errors_list["password_err"] = "Password is required";
    }
}
```

Приклад коду валідації даних отриманих через POST запит

Саме тут ми і використали нашу функцію для обробки даних і правильну перевірку, де строки з умови `if ($_SERVER["REQUEST_METHOD"] == "POST")`.

Означає що ми перевіряємо чи виконався POST запит. Після цього ми перевіряємо чи існує ключ registration-nicename і чи не порожній він, ЯКЩО НІ – ЗАПИСУЄМО ДАНІ В ЗМІННУ \$registered_nicename за допомогою нашої функції яку ми задекларували раніше. Таку саму ситуацію можна побачити і з паролем але в умові ще перевіряємо кількість символів в ньому це для того щоб встановити мінімальну кількість символів для користувача. Після цього треба перевірити дані на регулярні вирази, якщо брати приклад з номером телефону, або поштову скриньку то нам треба встановити перевірки на кількість символів і на жорсткість перших 3 символів “+380” для українських номерів. Для того щоб додати можливість переключати номер за країнами та регіонами – ми можемо створити селект за допомогою HTML та вписати туди опції які матимуть значення перших 4х цифр номерних кодів різних країн, але для цього треба попередньо створити масив з цими значеннями і кожного разу перевіряти через регулярні вирази чи існує такий ключ в нашій колекції

```
if (preg_match('/^\+380\d{9}$/', $registered_phone)) {  
    echo "Valid Ukrainian phone number.";  
} else {  
    echo "Invalid Ukrainian phone number.";  
}
```

Перевірка номеру за допомогою регулярного виразу

Цей код означає що дані в нашій змінній ми перевіряємо перші 4 символи чи строго вони відповідають строці +380 а потім перевіряємо щоб було строго 9 символів.

```

$conn = new mysqli($servername, $username, $password, $dbname);

if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

$sql = "CREATE TABLE users (
    id INT AUTO_INCREMENT PRIMARY KEY,
    name VARCHAR(50) NOT NULL,
    pass VARCHAR(100) NOT NULL,
    phone_number VARCHAR(20) NOT NULL
)";

$stmt = $conn->prepare($sql);

if ($stmt === FALSE) {
    echo "Error preparing statement: " . $conn->error;
} else {
    if ($stmt->execute() === TRUE) {
        echo "Table users created successfully";
    } else {
        echo "Error creating table: " . $conn->error;
    }
}

```

MYSQL запит до бази даних

Цей фрагмент демонструє нам як треба починати роботу з нашою базою даних. Тут ми перевіряємо чи існує підключення до бази даних (далі БД). Якщо ні – ми перериваємо виконання коду і видаємо помилку яку нам поверне перевірка. Потім ми підготовуємо запит за допомогою метода `prepare` класу `mysqli` і робимо останню перевірку чи існує таке підключення і якщо так – робимо перевірку на коректність запиту і виконуємо його методом `execute` класу `mysqli`.

Після створення нашої таблиці в БД ми повинні автоматизувати запис даних в неї. В нашому випадку ми записуємо три величини

- 1 – Ім'я
- 2 – Пароль
- 3 – номер телефону

```
$sql = "INSERT INTO users ($registered_nicename, $registered_password, $phone_number) VALUES (?, ?, ?)";  
  
$stmt = $conn->prepare($sql);  
$stmt->bind_param("sss", $new_name, $new_pass, $new_phone_number);  
if ($stmt->execute() === TRUE) {  
    echo "New user inserted successfully";  
} else {  
    echo "Error inserting user: " . $conn->error;  
}  
  
$stmt->close();  
$conn->close();
```

Приклад створення і занесення нового користувача в БД

Тут використовується та сама логіка що і при створенні таблиці БД, але відрізняється запитом аргументу метода `prepare`, де підставляємо раніше записані провалідовані значення полів передані методом `POST`.

В цілому вся робота з БД проходить майже в одному порядку, але різні технології потребують різних видів полів і даних в них а також бувають різні види запитів для маніпуляцій з даними, але це не стосується нашої теми. Ще можна додати що рівень знань розробника в сфері БД дуже сильно залежить від вміння правильно розділяти дані та взаємопов'язувати таблиці між собою. Так на нашому проекті за кожним працівником буда зав'язана роль і його унікальний ідентифікатор. І при видаленні користувача або працівника усі дані пов'язані з його ідентифікатором будуть видалятися разом, така властивість називається каскадуванням за ідентифікатором.

Останнє що я забув згадати це шифрування. Тут все доволі просто, PHP має функцію `md5` яка шифрує дані і їй можна додавати різні аргументи, флаги та константи, які будуть впливати на довжину та вид зашифрованої строки.

Більш детальніше про проект на прикладі фонду ВІДВАЖНІ:

є два засновника: один відповідає за зовнішні фактори (інвестори, гроші, гранти, партнери), а інший — за внутрішні (волонтери, налагодження роботи в команді, розподіл ролей та відповідальності).

У роботі Фонду є два напрямки:

- Проектна діяльність;

- Гуманітарна допомога.

Проектна діяльність - це реалізація різноманітних заходів: отримання грантів та їх реалізація, допомога організаціям у зборі коштів або підтримці таких зборів, чи проведення курсів з медіаграмотності для підлітків. Усі ці процеси завжди супроводжуються збором даних (дітей, батьків, згоди батьків на участь їхніх дітей у таких курсах/заходах, збору зворотного зв'язку від дітей та батьків через форми, де вони також вносять свої контактні дані).

Гуманітарна допомога – є літні люди, яким Фонд допомагаємо їжею та спеціальною гігієною. За кожною парою волонтерів закріплений маршрут та люди, яким потрібно протягом 5 днів щомісяця роздавати ці продукти чи гігієну, складати звіт на місці (кому видали чи кому передали, бо частіше всього родичі забирають) і по приїзду скласти звіт, скільки всього роздали і скільки залишилося/не взяли.

Виходячи з цієї інформації поетапне створення проекту буде таким:

- 1) Створення архітектури
- 2) Дизайн
- 3) Створення таблиці з ролями. У кожного користувача буде своя роль, всього їх 4.
 - 1- Суперадміністратор, технічний користувач, в цілому для підтримки технічної частини проекту, а не для взаємодії з його елементами.
 - 2- Власник, користувач з доступом до всіх взаємодій і даних на сайті.
 - 3- Волонтер. Працівник, який матиме власну статистику та список завдань та адрес на найближчі виїзди.
 - 4- Клієнт – користувач який матиме доступ до фідбеку(тут він зможе описати проблеми які виникли, зауваження чи скарги.
- 4) Створення форм реєстрації, відновлення паролю та авторизації для звичайних користувачів (користувачів з іншими ролями буде створювати або власник, або суперадмін)
- 5) Створення адмін панелі – дизайн та елементи в яких будуть виводитися:

- 1- дані з нашої БД про працівників і їх прокладену роботу.
- 2- Фінансовий запас фонду
- 3- Виконані благодійні проекти
- 4- Відгуки
- 5- Форма для додавання нових волонтерів та нових маршрутів та завдань
- 6- Хронологія подій
- 6) Створення меню волонтера
 - 1- Інформація про завдання
 - 2- Маршрути
 - 3- Закриті маршрути та виконані завдання
 - 4- Інформація про перелік необхідних документів та інша інформація фонду
- 7) Верстка основних сторінок проекту
- 8) Реєстрація нового типу постів, який буде показувати проекти фонду та описувати його діяльність і основну місію
- 9) Прив'язка платіжної системи для донатів (для благодійного фонду це може бути PayPal гаманець, створений за допомогою ПриватБанк Бізнес інтерфейс для поповнення рахунку або посилання на поповнення Monobank банку.
- 10) Девелопінг проекту з локального серверу на хостинг, додаючи усі правила безпеки та підтримку, встановлення та підключення та взаємностей на сервер необхідних технологій для нормального функціонування сайту.

Висновки до 2-го розділу

Для того щоб виконати кожен пункт списку потрібні вище згадані технології та приклади коду, скриптів. Єдина особливість – різноманітність даних які залежать від складності та структури елементу. Звичайно що фронт частина сайту дуже залежить саме від бажань клієнту та видіння з майстерністю дизайнера. Зазвичай дизайнер з меншими навичками в своїй професії намагається заповнити пробіли своїх знань безглуздими та недоречними анімаціями, фотографіями чи елементами, які лише будуть навантажувати сайт, і саме це 90% фронт частини проекту. Щодо бекенд частини то вона завжди залежить від даних і необхідного мінімуму функціональності, але це все лише варіативність технологій що використовуються на проекті та їх правопис.

Аналіз методів захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії, показав що неможливо віддати перевагу якомусь одному методу захисту персональної інформації. Усі методи захисту персональних даних цілеспрямовано впливають на захист інформації, але захист в повному обсязі неможливо забезпечити тільки одним методом. Спираючись на аналіз методів захисту персональних даних, нами запропоновано удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії.

Напрямок подальшого дослідження можливий у форматі: аналіз та удосконалення методів атак не тільки за допомогою соціальної інженерії а також за допомогою інших методів та типів. Створення математичної моделі захисту персональної інформації, наприклад.

Розглянуто та охарактеризовано проблему стрімкого розвитку сучасних технологій, через які є актуальне питання щодо захисту персональних даних користувачів мережі Інтернет. Проаналізовано сучасний стан забезпечення захисту персональних даних за вимогами українського законодавства та Загального регламенту про захист персональних даних (англ. *General Data*

Protection Regulation, GDPR). Визначено, які саме дані належать до персональних даних та чому підлягають захисту. З'ясовано, що персональні дані – це вид інформації з обмеженим доступом, тому обробляти ці дані потрібно тільки у системах, на яких встановлено комплексну систему захисту інформації, що має сертифікат відповідності.

РОЗДІЛ 3. ПЕРЕВІРКА ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОГО АЛГОРИТМУ.

З розвитком новітніх технологій і різноманітних застосунків, соцмереж і публічних каналів у месенджерах головним боєм благодійних організацій став захист персональних даних користувачів/учасників процесу. Запропонований алгоритм включає в себе:

1. Законність, справедливість і прозорість

Законність – у Фонді має бути вагома причина, щоб обробляти персональні дані. В першу чергу, це в тому разі, коли необхідна конкретна інформація для надання конкретної допомоги. Справедливість – фонд не може навмисно приховувати мотиви збору даних. А його підопічні та волонтери не повинні перейматися за те, що на неправомірному використанні їхні дані. Прозорість – чіткість, відкритість і чесність щодо того, як і чому фонд обробляє персональні дані.

2. Обмеження мети збору даних

Цей принцип GDPR означає, що дані «збираються лише з визначеною, явною і законною метою».

3. Мінімізація даних

Фонд повинен збирати тільки ті дані, які потрібні для досягнення своєї мети.

4. Точність

Фонд повинен забезпечувати точність даних, які збирає і зберігає. Він має вживати заходів, аби виправляти, оновлювати чи видаляти неправильні чи неповні дані.

5. Обмеження терміну зберігання

Фонд повинен обґрунтувати тривалість зберігання даних. Йдеться про крайні терміни зберігання даних, щоб відповідати політиці обмеження зберігання.

6. Цілісність і конфіденційність

Фонд вимагає підтримувати цілісність і конфіденційність даних, захищаючи їх від внутрішніх і зовнішніх загроз. Необхідний захист даних від

несанкціонованої або незаконної обробки та випадкової втрати, знищення або пошкодження.

7. Підзвітність

Відповідно до принципу підзвітності Фонд повинен мати відповідну документацію, що буде доказом дотримання принципів обробки даних. Регулятор може вимагати ознайомлення із цією документацією.

Спираючись на аналіз методів захисту персональних даних, нами запропоновано удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії.

3.1. АНАЛІЗ ЕФЕКТИВНОСТІ ТА ОПТИМІЗАЦІЇ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ОСНОВІ ЗАПРОПОНОВАНОГО АЛГОРИТМУ

Смартфон кожної людини містить масу персональної інформації – фото, контакти, листування, історія пересувань, банківські картки з можливістю NFC-оплат. Про захист всього цього піклується як сам користувач, так і виробники смартфонів, операційних систем і додатків.

Когось з користувачів захист персональних даних хвилює більше, когось – менше. Але вже точно абсолютно байдужих до цього питання людей не існує.

Гострою проблемою сьогодення стало повномасштабне вторгнення, яке призвело до великої кількості людей, що стали незахищеними. Організації почали допомагати, привозити, об'єднувати і, звичайно, це все відбувалось за підтримки міжнародних організацій, які потребували звітності, яка можлива тільки за умови надання персональних даних людей.

Зі швидким розвитком інтернету, ускладненням його архітектури, зростанням впливу та збільшенням кількості зловживань із боку недобросовісних користувачів у ЄС постало питання ґрунтового перегляду регуляторних норм. У 2018-му інституції ЄС ухвалили Загальний регламент про захист персональних даних, який замінив Директиву 95/46/ЄС. На відміну від директиви, яку країни ЄС мали інтегрувати у своє законодавство.

Водночас держава намагається захищати громадян юридично та технічно. Відповідно до законодавства, розпорядники зобов'язані захищати персональні дані в автоматизованих системах або картотеках. Крім цього, що стосується державних органів, всі інформаційні системи, які зберігають персональні дані, повинні мати комплексну систему захисту та атестат відповідності.

У Благодійній Організації «Благодійний фонд «ВІДВАЖНІ!»» прагне зробити все можливе, аби виправдати довіру учасників процесу і відповідальне ставлення до особистої інформації, в тому числі, персональних даних, не є винятком. Фонд дбайливо оберігає і захищає особисту інформацію відвідувачів Веб-Сайтів, включаючи веб-сайти для мобільних пристроїв, («Сайти») та користувачів мобільних додатків («Мобільні додатки»), особливо дитячих.

Види інформації, яку Фонд отримує:

- Поширення особистої інформації.
- Повідомлення про Конфіденційність особистої інформації дитини.
- Доступ.
- Файли «cookie».
- Посилання на інші Сайти.
- Внесення змін до Політики конфіденційності.
- Наші контакти.

1. Види інформації, яку Фонд отримує, і для чого вона потрібна

Інформація, яку Ви надає користувач послуг благодійної організації:

фонд збирає особисту інформацію, таку як ім'я, по-батькові та прізвище, поштова адреса, адреса електронної пошти та телефон. Фонд збирає особисту інформацію для того, щоб отримати відгук про Онлайн-сервіс та благодійну допомогу чи щоб мати можливість зареєструватися для участі в наших благодійних акціях. Учасник має право не надавати цю інформацію, але в цьому випадку Сайт чи Мобільний додаток можуть працювати неправильно, або деякі функції можуть бути недоступними.

До того ж, коли користувач відвідує Веб-Сайт чи Мобільний додаток, Фонд може отримувати певну інформацію автоматично. Така інформація може включати IP-адресу, дані про операційну систему комп'ютера/мобільного пристрою та тип браузера, тип мобільного пристрою, унікальний ідентифікатор пристрою (UDID) чи ідентифікатор мобільного обладнання (MEID) мобільного пристрою, адресу веб-сайту, на якому містилось посилання на нас (якщо є), та сторінки, які відвідали на Веб-Сайтах. Фонд може використовувати цю інформацію для того, щоб здійснювати керування, обслуговування та налаштування Онлайн-сервісу, а також щоб надавати послуги типу технічної підтримки

Мобільні додатки та мобільні версії Сайту можуть отримувати точну інформацію щодо місцезнаходження мобільного пристрою, використовуючи технології визначення місцезнаходження, такі як GPS, Wi-Fi, Bluetooth чи відстань до найближчої вишки стільникового зв'язку. Благодійна Організація використовує цю інформацію для надання послуг, які залежать від місцезнаходження, наприклад при пошуку найближчих місць проведення благодійних акцій Фонду чи визначенні спеціальних пропозицій, які можуть бути цікаві, чи для персоналізації взаємодії з Фондом. У випадку більшості мобільних пристроїв є змога відкликати дозвіл, який надали Фонду, для отримання інформації про місцезнаходження через налаштування пристрою учасника процесу. Якщо ж учасник бажає, щоб Фонд видалив отриману інформацію про місцезнаходження, потрібно надіслати Фонду повідомлення електронною або звичайною поштою за адресою, що вказана на сайті. Після видалення додатки можуть працювати неправильно, і що Фонд може бути змушений зберігати деяку інформацію через вимоги законодавства.

БФ «ВІДВАЖНІ» може поширювати особисту інформацію компаніям та залежним структурам, які виступають як волонтери-партнери Фонду. Звичайно, будь-яке використання такої інформації відбувається відповідно до політики Фонду. Час від часу з дозволу учасників процесу Фонд буде надсилати звіти, відгуки про проведені благодійні акції та благодійну допомогу, маркетингову інформацію щодо нових благодійних акцій і т. д.

БФ не продає, не передає та не повідомляє особисту інформацію третім сторонам. Однак, з дозволу учасників, Фонд буде іноді надсилати маркетингову інформацію від імені якогось із волонтерів-партнерів щодо допомоги чи благодійних акцій, які надаються і які можуть зацікавити учасників процесу. Додаток може запитати, чи бажають учасники отримувати маркетингові матеріали від волонтерів-партнерів БФ. Якщо учасники погодяться отримувати такі матеріали, БФ не буде повідомляти вашу особисту інформацію цим партнерам, а лише буде надсилати матеріали чи листи електронною або звичайною поштою від імені цих волонтерів-партнерів.

БФ зберігає за собою право використовувати чи повідомляти будь-яку інформацію, якщо це вимагається будь-яким законом, нормативно-правовим актом чи правовою вимогою, з метою захисту цілісності Онлайн-сервісу, для виконання ваших запитів, чи з метою сприяння будь-якому розслідуванню з боку правоохоронних органів чи розслідуванню з метою забезпечення громадської безпеки.

Персональні дані відвідувачів використовуються для полегшення користування Сайтом відвідувачів, обліку їх інтересів і переваг при здійсненні політики Благодійної Організації, а також для аналізу поведінки користувачів, в тому числі і в роботі з контрагентами в сфері реклами. Персональні дані використовуються відповідно до таких Законів України: Закон України "Про захист персональних даних", Закон України «Про інформацію», Закон України «Про рекламу», Закон України «Про благодійну діяльність та благодійні організації».

БФ розуміє, наскільки важливо для відвідувачів та користувачів Онлайн-сервісу зберігати в таємниці особисту інформацію. Особливо уважно Фонд ставиться до захисту особистої інформації дітей, котрі відвідують чи користуються Онлайн-сервісом. Це Повідомлення про Конфіденційність особистої інформації дитини розроблене для того, щоб відповісти на питання стосовно принципів роботи Фонду з особистою інформацією, яку Фонд отримує через Онлайн-сервіс від дітей до 14 років.

Фонд не пропонує дистанційні продажі, жодна інформація, яка розміщена в запропонованому додатку, не є публічною офертою відповідно до чинного законодавства України.

На Сайті пропонується багато додаткових елементів, таких як ігри чи книги-розмальовки, які не вимагають від дитини повідомлення жодної особистої інформації. Однак, іноді Фонд отримує від дитини особисту інформацію, таку як адреса електронної пошти, в процесі взаємодії.

Наприклад: Фонд може отримати адресу електронної пошти дитини для того, щоб повідомити їй/йому про перемогу або поразку в конкурсі чи розіграші. В цьому випадку, Фонд надсилає дитині повідомлення на вказану адресу електронної пошти. Фонд не буде зберігати ці дані чи використовувати їх з будь-якою іншою метою.

Фонд може отримати адресу електронної пошти дитини для того, щоб відповідати на разові запити дитини, наприклад, надіслати дитині заставку для екрану. В такому випадку Фонд видаляє адресу електронної пошти з системи

одразу ж після відправлення відповіді і не використовуємо адресу для жодних інших цілей.

Фонд не збирає іншу особисту інформацію від дітей до 14 років, таку як поштова адреса чи номер телефону, без дозволу батьків чи опікунів. Якщо Фонду буде необхідний дозвіл батьків чи опікунів, представники попрость надати адресу електронної пошти батьків чи опікунів, щоб надіслати їм повідомлення про принципи роботи з інформацією та/або попросити батьків чи опікунів надати свій дозвіл.

Благодійна Організація ніколи не вимагає від дитини надавати більше особистої інформації для участі в будь-якій програмі, ніж це дійсно необхідно для взяття участі в такій програмі.

Фонд використовує адресу електронної пошти, вказану дитиною, для того, щоб відповідати на її/його запити чи повідомляти їй/йому про перемогу або поразку в конкурсі чи розіграші, в якому дитина брала участь. Фонд використовує адресу електронної пошти батьків чи опікунів для того, щоб надіслати їм повідомлення про принципи роботи з інформацією та/або попросити батьків чи опікунів надати свій дозвіл.

Фонд може передавати особисту інформацію дитини третім сторонам виключно в мірі, об'єктивно необхідній для того, щоб захистити безпеку чи цілісність Онлайн-сервісу, для застосування запобіжних заходів проти притягнення до відповідальності чи для сприяння судовим процесам або запитам інших державних органів; чи у випадках, коли, на наш погляд, необхідно надати таку інформацію задля попередження завдання фізичної шкоди чи фінансових збитків, чи у зв'язку з розслідуванням стосовно підозрілої чи фактичної незаконної діяльності.

Фонд також можемо передавати особисту інформацію, надану дітьми, постачальникам, які надають послуги Благодійної Організації. Ці послуги можуть включати в себе хостинг Сайту, надання Благодійної Організації послуг технічної підтримки, виконання запитів чи організацію розіграшів або конкурсів. Такі постачальники зобов'язані зберігати конфіденційність особистої інформації, яку їм надається Фондом.

Учасники процесу повністю контролюють всю особисту інформацію, яка надається через запропонований додаток. В будь-який час, коли учасник вирішить редагувати особисту інформацію, яку отримали, чи якщо учасник бажає змінити свої налаштування стосовно інформації, яку отримує від Фонду чи від імені волонтерів-партнерів, учасник може повідомити Фонд про це, відправивши листа електронною чи звичайною поштою.

Файл «cookie» – це текстовий файл, який веб-сайти надсилають на комп'ютер або інший пристрій відвідувача з підключенням до мережі інтернет виключно для того, щоб ідентифікувати браузер користувача або зберігати інформацію чи налаштування в браузері. Як і більшість веб-сайтів, Благодійна Організація використовує файли «cookie» для різноманітних цілей з метою поліпшення умов активності в інтернеті. Наприклад, Фонд відслідковує загальну кількість відвідувачів Сайту на сукупній анонімній основі. Фонд також може застосовувати файли «cookie» щоб запам'ятати учасника процесу,

коли повертається на Сайт, а також щоб допомогти налаштувати роботу з Онлайн-сервісом Благодійної Організації. В таких випадках Фонд може прив'язувати особисту інформацію до файлів «cookie». Фонд, як і інші організації (наприклад, рекламні мережі), може збирати особисту інформацію про інтернет-активність відвідувачів в часі, в тому числі через сайти третіх сторін, при користуванні Онлайн-сервісом.

Так, відповідальна особа/підрозділ повинна здійснювати контроль за дотриманням працівниками володільця чи розпорядника політики приватності (наприклад, з метою моніторингу законності доступу до персональних даних переглядати журнал обліку операцій, пов'язаних з обробкою персональних даних), актуалізувати інформацію щодо потенційних ризиків, переглядати в разі потреби організаційні та технічні заходи захисту персональних даних, порядок їх обробки з метою зокрема приведення їх у відповідність до нових ризиків (чи мінімізації втручання в права особи на приватність, внаслідок такої обробки), доводити результати роботи до відома керівництва, підтримувати в актуальному стані документи. Правове регулювання та практичні аспекти регламентують порядок обробки персональних даних володільцем чи розпорядником:

- вживати заходів у разі виявлення порушення законодавства про захист персональних даних.

Якщо мова йде про порушення, що може мати серйозні наслідки для прав суб'єктів персональних даних, про це слід відразу доводити до відома керівництва та Уповноваженого, а також вживати/рекомендувати керівництву вжиття першочергових заходів, спрямованих на мінімізацію потенційних негативних наслідків.

Окрім того, в разі наявності такої можливості про це порушення слід повідомляти самого суб'єкта/ів персональних даних:

- ознайомлювати (організовувати процес ознайомлення) керівництво та працівників володільця із вимогами чинного законодавства про захист персональних даних, змінами до законодавства, актуальними питаннями обробки персональних даних у сфері діяльності володільця, організовувати відповідні навчання для працівників;
- взаємодія з Уповноваженим, що може проявлятися у таких основних напрямках: 1) консультації з приводу доцільності та порядку обробки персональних даних володільцем, отримання з цього приводу роз'яснень Уповноваженого;

2) отримання висновку щодо розробленого кодексу поведінки відповідно до ст. 27 Закону (у випадку, коли мова йде про роботу державного органу, органу місцевого самоврядування – направляти Уповноваженому для погодження проекти нормативно-правових актів, що стосуються питань обробки персональних даних);

3) співпраця в ході розгляду Уповноваженим звернень громадян (надання необхідних документів та інформації);

4) співпраця в ході проведення Уповноваженим перевірки володільця (забезпечення швидкого надання усієї інформації щодо обробки персональних даних володільцем, супровід в ході проведення перевірки, забезпечення вільного доступу до усіх приміщень, де здійснюється обробка персональних даних, та безпосередньо до інформації (і в тому числі персональних даних), що обробляється володільцем та інше);

5) забезпечення вчасного та повного виконання приписів Уповноваженого;

6) участь в освітніх, науково-практичних заходах, що проводяться Уповноваженим та працівниками.

ату;

7) участь в разі необхідності в громадських радах, що діють при Уповноваженому;

8) надання вузькоспеціалізованих консультацій працівникам Секретаріату Уповноваженого;

З метою виконання такого широкого спектру завдань відповідальна особа/підрозділ повинні користуватися відповідними правами, які необхідні для належного виконання ними своїх посадових

обов'язків, а саме право:

- безперешкодного доступу до приміщень, де здійснюється обробка персональних даних;
- доступу до всієї інформації та документів, що стосуються здійснення володільцем чи розпорядником обробки персональних даних, і в тому числі персональних даних, що містяться у базах даних володільця, журналу реєстрації обліку операцій, пов'язаних із обробкою персональних даних та інші;
- своєчасно отримувати повну інформацію щодо будь-яких операцій, пов'язаних з обробкою персональних даних, що здійснюються володільцем чи розпорядником;
- право безпосереднього звітування керівництву володільця чи розпорядника.

Для виконання вказаних вище завдань відповідальна особа/підрозділ повинні володіти відповідними навиками та статусом. Так, це повинна бути особа, яка володіє відповідною кваліфікацією у сфері захисту персональних даних та безпеки інформації. Для цього рекомендується наявність у неї відповідної освіти чи проходження такою особою відповідного спеціалізованого навчання.

Висновки до 3-го розділу

Росіяни в усі можливі (й не лише законні) способи збирають інформацію про громадських активістів, волонтерів, правозахисників, журналістів, голів об'єднаних територіальних громад, щоби потім, після окупації міст і сіл, знаходити їх і знищувати. Так, під час окупації Херсона колаборанти спільно з російськими військовими розшукували активних людей, які потенційно могли вести спротив і допомагати Збройним силам України. Звільнені від окупантів громади Харківщини відкрили численні історії про те, як росіяни знущалися, катували та вбивали проукраїнських людей.

Варіантів використання персональних даних багато. Починаючи від індивідуальних переслідувань — наприклад, як в окупованому Херсоні, коли переслідували активістів, журналістів, представників медіа, правозахисників, — так і для того, щоби планувати воєнні операції. Знання статистичної інформації є дуже корисними при будь-якому плануванні, зокрема і воєнних операцій. Можна також перешкоджати конкретним людям, які є активістами чи волонтерами, погрожувати їм, якщо в них є родичі на тимчасово окупованих територіях, а вони волонтерять на підконтрольній Україні території.

Тому що, по суті, це благодійна допомога, яка не має оподатковуватися. Хоча інші гроші, які заходять на приватні картки, часто є нелегальним підприємництвом. Тобто коли люди намагаються уникнути оподаткування шляхом просто прямих переказів оплати за якісь товари на їхню приватну картку. Для того, щоб волонтери не кваліфікувалися податковою службою як ті, хто незаконно отримує гроші, вони реєструються в Реєстрі волонтерів. Так податкова знає, що ця особа — волонтер і не проводить жодних фінансових махінацій.

Саме для уникнення таких проблем, метою цієї роботи є запропонувати необхідність створення систем захисту персональних даних БФ та перевіряти інформацію про діяльність організацій через відкриті онлайн платформи.

Що тут важливо? По-перше, реєстр є державним. За своєю суттю він нічим не відрізняється від, наприклад, «Дії» або Реєстру платників податків. Це відразу індикатор того, що він досить безпечний. На противагу, якщо громадські організації або фонди створюють свої реєстри, тут питання стоїть трохи гостріше.

З юридичної точки зору проблема виникає, коли організації не до кінця пояснюють отримувачам допомоги, яка мета збирання даних. Така ж проблема існує в розрізі отримання інформації про волонтерів, наприклад, коли їм хочуть надавати премії. Коли людям, чию інформацію збирають, не до кінця пояснюють мету, спосіб збирання даних і де їх можуть використати.

Для населення на окупованих та деокупованих територіях, як на прикладі БФ «ВІДВАЖНІ», який свою основну діяльність реалізовує на території Корсотенщині, що під білоруським кордоном, надзвичайно важливо намагатися не отримувати гуманітарну допомогу від держави-агресорки. Також не варто брати участь у так званих переписах населення на окупованих

територіях, які проводить держава-агресорка. Особливо важливо не розкривати дані про військовослужбовців, членів їхніх сімей, громадських активістів, журналістів, культурних діячів, правозахисників тощо. Тому що дуже часто такі переписи населення проводять саме з метою отримання цієї інформації. Так само варто дотримуватись базових правил кібербезпеки. Лабораторія цифрової безпеки розробила продукт, який називається «Як?». Це ресурс, який допомагає посилити цифровий захист акаунтів, налаштувати приватність, фільтри від спаму та небезпечних ініціатив на різних ресурсах, починаючи від браузерів і закінчуючи соціальними мережами та месенджерами.

ВИСНОВКИ І ПРОПОЗИЦІЇ

Відкритий інтернет, Google, соцмережі та інше, те, що індексується пошуковими системами, це приблизно 10% інформації в Інтернеті. Це те, що може кожен із нас знайти, маючи навички. У цьому нічого складного. Фактично, це та ж розвідка. Але за допомогою сучасних технологій, штучного інтелекту тощо можна швидко дізнатися про те, що, як і де відбувається. Це можуть бути Google-карти, фотографії, які є в мережі, відео чи пости.

Відповідно до частин першої, другої статті 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

З точки зору методології в проблемі захисту інформації від НСД слід виділити два напрями: забезпечення і оцінка захищеності інформації в АС, що функціонують; реалізація та оцінка засобів захисту, що входять до складу компонентів, з яких будується обчислювальна система АС (програмних продуктів, засобів обчислювальної техніки і т. ін.), поза конкретним середовищем експлуатації. Кінцевою метою всіх заходів щодо захисту інформації, які реалізуються, є забезпечення безпеки інформації під час її обробки в АС. Захист інформації повинен забезпечуватись на всіх стадіях життєвого циклу АС, на всіх технологічних етапах обробки інформації і в усіх режимах функціонування. Життєвий цикл АС включає розробку, впровадження, експлуатацію та виведення з експлуатації. [16]. Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних.

Персональні дані є важливим інструментом благодійної організації, так як з повномасштабним вторгненням їх кількість значно зросла, а відповідно і зріс попит на надання благодійної та волонтерської допомоги, що в свою чергу за саобою несе фіксування даних людей, що звертаються.

Саме тому, важливість теми, що досліджувалась є дуже актуальною, адже зберігання конфіденційності – це важливий рівень довіри, який організації втратити не можуть, а відповідно вони мають себе убезпечити усіма можливими інструментами. Такими інструментами може стати саме подібний застосунок, дія та алгоритми якого описані вище. Не менш важливим є і дотримання запропонованого технічного завдання для досягнення мети роботи.

Загрози персональним даним можна описати наступним чином -це загрози несанкціонованого зберігання, використання та поширення конфіденційних даних. За згодою суб'єкта персональних даних конфіденційна інформація може оброблятися і зберігатися розпорядником, мету в цей час визначає володілець даних.

Таким чином, володілець і розпорядник несуть відповідальність за дотримання конфіденційності довіреної їм інформації. Будь-які дані зберігаються в інформаційних системах, а отже, мова про загрози персональним даним, які зберігаються та обробляються в ІС (інформаційних системах). Усі загрози можна умовно поділити на такі, які можуть бути реалізовані внаслідок атак, та такі, які не залежать від атак. Загрози, які не пов'язані з цілеспрямованими атаками, можуть як призвести до втрати, спотворення або компрометації персональних даних суб'єкта, так і створити умови для їх використання зловмисниками.

Такими загрозами можуть бути:

- такі, що не пов'язані з діяльністю людини: стихійні лиха та природні явища (землетруси, повені, урагани тощо);

- загрози соціально-політичного характеру: страйки, диверсії, локальні конфлікти, війна, що супроводжуються нападом на об'єкт, що містить ресурси інформаційної системи, тощо;
- помилкові дії та/або порушення персоналом та користувачами інформаційної системи вимог до відповідної експлуатаційної, організаційної, технічної чи іншої документації;
- загрози антропогенного характеру, наприклад: аварії та різного роду несправності та перешкоди, що призводять до порушень і збоїв у роботі апаратних компонентів інформаційної системи.

Закон України “Про інформацію” [1] окреслює конфіденційну інформацію як інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Захист від загроз, які не залежать від атак, регулюється інструкціями, розробленими та затвердженими уповноваженими службами розпорядника персональних даних, з урахуванням специфічних умов функціонування інформаційної системи, а також чинних нормативних документів. Захист від загроз, які можуть бути реалізовані внаслідок атаки, повинен забезпечуватися за допомогою захисних заходів і засобів, які використовуються інформаційною системою і призначені переважно для протидії атакам. Атака соціальної інженерії має спільну структуру. Вони відбуваються в один або кілька кроків

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Електронна енциклопедія Wikipedia. Англomовна версія [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/Open-source_intelligence
2. Електронна енциклопедія Wikipedia. Англomовна версія [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/Intelligence_collection_management
3. Hamilton, B. The DNI's Open Source Center: An Organizational Communication Perspective / B. Hamilton // International Journal of Intelligence and CounterIntelligence [Електронний ресурс]. – Режим доступу: http://www.oss.net/dynamaster/file_archive/110802/98532478899216432d3d76e2f9d4534c/2011-0802%20Dr.%20Bean%20IJC%20Open%20Source%20Center.pdf
4. Intelligence Community Directive (ICD 301), July 2006 [Електронний ресурс]. – Режим доступу: http://www.dni.gov/electronic_reading_room/ICD_301.pdf
5. Башмаков А.И. Интеллектуальные информационные технологии: Учебн. пособие / А.И. Башмаков, И.А. Башмаков. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2005. – 304 с.
6. Bem, M. V., Gorodisky, I. M., Sutton, G., & Rodionenko, O. M. (2020). Protection of personal data: legal regulation and practical aspects. Kyiv: KIS, Published by the Council of Europe. F-67075 Strasbourg Cedex.
7. Корченко А.Г. Несанкционированный доступ к компьютерным системам и методы защиты. Учебное пособие. К.: КМУГА.- 1998.-116 с.
8. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
9. GDPR. (2021). Ofitsiine Vydannia. Retrieved from: <https://gdpr-info.eu/chapter-4>. [In Ukrainian].

10. The Global Internet Phenomena Report September 2019 [Електронний ресурс]. – Режим доступу до ресурсу: https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/Internet%20Phenomena/Internet%20Phenomena%20Report%20Q32019%2020190910.pdf. – Назва з екрана.
11. «The Global Internet Phenomena Report September».
12. Lehka, O. V. (2021). Actual issues of personal data protection: domestic and international experience. *Legal position*, 2(31), 74–79, <https://doi.org/10.32836/2521-6473.2021-2.15>
13. Mengesa, F., Latzob, T., Vielbertha, M., Sobolad, S., Pöhlsc, H., Taubmannc, B., ..., Pernula, G. (2021). Towards GDPR-compliant data processing in modern SIEM systems. *Computers & Security*, 103. <https://doi.org/10.1016/j.cose.2020.102165>
14. Salashnik, R. O., & Shabatura, M. M. (2021). Requirements for personal data protection under the rules of GDPR. *Proceedings the XVI International Conference Problems and prospects for the development of life safety system*, 259–261.
15. Nakaz. (2021). Nakaz Ministerstva Yustytysii Ukrainy Vid 30.12.2011. № 3659/5 "Pro Zatverdzhennia Typovoho Poriadku Obrobky Personalnykh Danykh U Bazakh Personalnykh Danykh". Retrieved from: <https://zakon.rada.gov.ua/laws/show/z0001-12#Text>. [In Ukrainian].
16. Anti-Phishing Phil. <https://www.cmu.edu/iso/aware/phil/index.html>.
17. Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., Biehun, A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security (IJCNIS)*
18. Черняк, А. М., Прозоров, А. Ю. (2019). Аспекти запобігання правопорушенням у сфері використання банківських платіжних карток під час проведення безконтактних й інтернет-платежів та їх кваліфікація. *Naukovij visnik Nacional'noi akademii vnutrisnih sprav*

19. Yoshihara, T. (2001). Chinese information warfare: A phantom menace or emerging threat? Strategic Studies Institute, U.S. Army War College.
20. Хорошко, В.О., Хохлячова, Ю.Є. (2016). Information war. Mass media as an instrument of information influence on society. Part 1. Ukrainian Scientific Journal of Information Security.