Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань _____ 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність _____ 125 Кібербезпека
(код і назва спеціальності)

освітня програма _____ Кібербезпека
(назва освітньої програми)

на тему: «Рекомендації щодо захисту інформаційної безпеки особистості»

Виконавець: студентка IV курсу, групи КБ-42

_____ **Олександра ТЕРЕЩЕНКО**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Сергій ДАКОВ	

Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності _____ 125 Кібербезпека
(код і назва спеціальності)

освітньої програми _____ Кібербезпека
(назва освітньої програми)

Студентці __ **КБ-42** **Олександри Володимирівни Терещенко**
(група) (прізвище ім'я по батькові)

Тема дипломної роботи Рекомендації щодо захисту інформаційної безпеки особистості

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

Методики захисту інформації

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теоретичною основою інформаційної безпеки особистості, проаналізувати нормативно-правове забезпечення, визначити основні загрози та розробити модель порушника безпеки людини в інформаційному середовищі, розробити технічні рекомендації для захисту інформаційної безпеки особистості

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації щодо захисту безпеки особис-

тості в інформаційному середовищі для самої особистості.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ Сергій ДАКОВ
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Олександра ТЕРЕЩЕНКО
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021 – 22.01.2022	*виконано*
2	Аналіз літератури	29.01.2022 – 11.02.2022	*виконано*
3	Аналіз нормативно-правової бази	12.02.2022 – 15.02.2022	*виконано*
4	Аналіз теоретичної складової	16.02.2022 – 04.03.2022	*виконано*
5	Дослідження вразливостей та загроз	05.03.2022 – 21.03.2022	*виконано*
6	Побудова моделі порушника на основі можливих загроз.	22.03.2022 – 08.04.2022	*виконано*
7	Розробка рекомендацій щодо захисту інформаційної безпеки особистості	09.04.2022 – 10.05.2022	*виконано*
8	Оформлення пояснювальної записки	11.05.2022 – 27.05.2022	*виконано*
9	Підготовка до захисту дипломної роботи	28.05.2022 – 13.06.2022	*виконано*

Завдання видав _____ Сергій ДАКОВ
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Олександра ТЕРЕЩЕНКО
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка: 52 сторінки, 4 рисунки, 30 літературних джерел.

Метою роботи є розробка технічних рекомендацій для забезпечення захисту інформаційної безпеки особистості.

Для досягнення мети необхідно виконати наступні задачі:

- проаналізувати теоретичну складову інформаційної безпеки особистості;
- проаналізувати нормативно-правову базу з питання інформаційної безпеки особистості;
- розробити модель порушника інформаційної безпеки;
- розробити рекомендації для забезпечення інформаційної безпеки особистості.

Об'єктом дослідження є процес захисту даних особистості у інформаційному середовищі.

Предметом дослідження в даній роботі є методи, засоби і методики захисту інформаційної безпеки особистості.

Під час дипломного проектування було використано наступні *методи дослідження:*

- інтелектуальний аналіз літературних джерел;
- порівняння та метод теоретичного узагальнення ;
- вивчення та узагальнення різних практик захисту.

В роботі проведено аналіз теоретичної складової інформаційної безпеки, нормативно-правового забезпечення, загроз та можливих методів захисту інформаційної безпеки особистості.

Запропоновано модель класифікації середовища особистості відповідно можливих загроз безпеці людини відповідно.

Побудовано модель порушника інформаційної безпеки особистості.

Розроблено загальні практичні рекомендації для забезпечення захисту інформаційної безпеки особистості на основі моделі порушника.

Практичне значення роботи полягає у використанні запропонованих рекомендацій для підвищення рівня власної інформаційної безпеки для кожної людини.

Результати, здійснених у дипломній роботі досліджень, можуть бути використані для поширення серед різних груп населення, з метою підвищення загального рівня обізнаності щодо загроз інформаційної сфери та можливостей захисту від цих загроз

Напрямки подальших досліджень:

- побудова захищеного середовища для громадян;
- розробка програм для автоматизації процесу захисту інформаційної безпеки.

Ключові слова: ЗАГРОЗИ, ІНФОРМАЦІЙНА БЕЗПЕКА ОСОБИСТОСТІ, ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО, МОДЕЛЬ ПОРУШНИКА БЕЗПЕКИ, ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА, ІНФОРМАЦІЙНО-ТЕХНІЧНА БЕЗПЕКА

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

API	–	Application Programming Interface
VPN	–	Virtual Privat Network (Приватна віртуальна мережа)
(D)DoS	–	(Distributed) Denial-of-Service
IoT	–	Internet of things (Інтернет- речей)
ІБ	–	Інформаційна безпека
ІКТ	–	Інформаційно-комунікаційні технології
ПЗ	–	Програмне забезпечення
ПК	–	Персональний комп’ютер
ОС	–	Операційна система

ЗМІСТ

ВСТУП

Аналіз соціальних процесів останніх років дозволяє говорити про наближення нашого суспільства до глобального інформаційного суспільства.

Кількість загроз інформаційні безпеці зростає пропорційно поширенню і збільшенню впливу інформаційних технологій на різні складові людської життєдіяльності. Інформаційна безпека має найбільше значення серед проблем інформаційних проблем окремих громадян та суспільства в цілому, а також на державному рівні. Її реалізація та забезпечення виконується державними апаратом, як складової національної безпеки. Кількість суб'єктів забезпечення в цій сфері збільшується дуже стрімко, але найменш захищеними досі є потреби особистості.

З розвитком інформаційного середовища, людина стає все більш незахищеною та «відкритою» для інших людей. Використовуючи різні засоби і методи, можна отримати доступ до великої кількості різних даних, що стосуються певної особи. Ця інформація може бути використана іншими особами чи групам осіб абсолютно з різними цілями. В інформаційних суспільних відносинах людина може брати участь як суб'єкт (наприклад, відносини щодо доступу до інформації, право на приватність тощо), може бути об'єктом (відносини щодо інформаційної безпеки), і навіть – засобом (відносини щодо маніпуляції свідомістю).

На мою думку, рівень захисту інформаційної безпеки особистості залежить в першу чергу від самої особистості. Тільки невелика частина населення здатна захистити себе. Тому дослідження проблем інформаційної безпеки особистості зараз є дуже актуальним питанням.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ

1.1 Поняття інформаційної безпеки

Питання інформаційної безпеки треба розглядати з декількох ракурсів. Зараз, в наукових виданнях немає не описано єдиного підходу до цього поняття. Його можуть визначати як стан, процес, діяльність чи функцію.

Інформаційна безпека це складова інформаційного середовища. Вона стосується різних рівнів, а саме людини, суспільства та держави. Тобто вона направлена на забезпечення захисту інформаційних ресурсів та їх суб'єктів. Зміст поняття залежить від області застосування, та розкривається у діяльності людини, наукових дослідженнях, а також у законодавчих актах.

Нижче наведено декілька визначень з наукової літератури та ті, що закріплені на законодавчому рівні:

1) Інформаційна безпека – це стан, на основі якого визначається захищенність інформаційного середовища на суспільному рівні, та забезпечується користування цим середовищем, відповідно до пріоритетів його суб'єктів.

Інформаційне середовище - це область діяльності, що основана на створенні, обробці та використанні інформації .

2) З іншого боку, інформаційна безпека – це рівень захищеності потреб особи, суспільства й держави в інформаційній сфері, що забезпечує їх взаємодію незалежно від можливих загроз інформаційного середовища. За рівнем інформованості визначають адекватність оцінки реальності суб'єктами та обґрунтованості їх рішень.

3) Інформаційна безпека – складова безпеки держави на національному рівні. Ця складова направлена на управління ризиками державних і недержавних інституцій та суспільства.

На рівні національної безпеки, інформаційна повинна забезпечувати:

- цілісність та суверенітет держави в інформаційному середовищі;

-забезпечення різних аспектів інформаційної сфери: використання нових технологій, контроль поширення недостовірної інформації про Україну та її розповсюдження;

-привертання уваги через використання засобів масової інформації про проблеми та явища, які становлять загрозу національній безпеці держави;

-забезпечення прав громадян на вільний доступ до інформації, унеможливлювання впливу органів державного регулювання на засоби масової інформації та дискримінації, що стосується інформаційної сфери;

-реалізація комплексу заходів, направлених на захист інформаційного простору на національному рівні та попередження створення монополії у цій сфері.

4) Відповідно до інформаційного права, інформаційна безпека це сторона інформаційних відносин, яка розглядаються у межах інформаційного законодавства, з метою захисту життєвонеобхідних суспільних та державних інтересів. В цій області увага акцентується на ризиках таких інтересів і можливостях їх усунення юридичними засобами.

5) Інформаційна безпека - це рівень захисту інтересів особистості, суспільста та країни, що має на меті запобігання завданню шкоди через неповну чи несвоєчасну інформацію, негативних інформаційних впливів; поганих наслідків при використанні інформаційних технологій; несанкціонованого розповсюдження, застосування і модифікації інформації

6) Інформаційна безпека- захист пріоритетних суспільних інтересів у інформаційній сфері, що включає в себе інформаційну та телекомунікаційну інфраструктуру, безпосередньо інформацію та її основні параметри. Головна різниця інформаційної безпеки полягає в тому, що вона є частиною безпеки національного рівня. З нею пов’язуються і інші складові національної безпеки, такі як укономічна, воєнна та політична.

Інформаційна безпека має такі рівні:

- правововий рівень — законодавче регулювання нормативно-правовими актами;

- адміністративний рівнь — дії державних структурних підрозділів;

- процедурний рівень;
- технічний рівень.

Види інформаційної безпеки:

1) Інформаційна безпека держави.

Це міра рівня захисту держави та стійкості її головних складових, наприклад економічної, наукової чи технічної тощо, відносно шкідливих впливів інформаційного середовища. Інформаційна безпека держави має на меті нейтралізацію подібних впливів.

Концепція інформаційної безпеки держави – це систематизований набір відомостей про варіанти можливих дій для забезпечення її інформаційної безпеки. В межах цієї концепції класифікуються загрози та ризики інформаційній безпеці у інформаційному середовищі; визначаються організаційні методи для забезпечення інформаційної безпеки; розробляються нові можливості для захисту.

2) Інформаційна безпека організації

Це спрямовані дії керівників та співробітників певної організації з метою для захисту інформаційного середовища, що необхідне для нормального функціонування та роботи організації.

3) Інформаційна безпека особистості.

Це захист однієї особистості чи групи від впливів інформаційної сфери, які здатні впливати на психічний стан чи стан сприйняття особи, та змінювати її поведінку.

На мою думку, інформаційна безпека не може розглядатися лише як одне конкретне поняття. Вона є властивістю та складовою інформаційного суспільства, процесом та результатом роботи людини, і спрямована на забезпечення захисту в інформаційній сфері.

На рисунку 1.1 представлене зображення взаємозв’язків різних видів інформаційної безпеки. Такий зв’язок означає те, що кожна складова тісно пов’язана зі іншою.

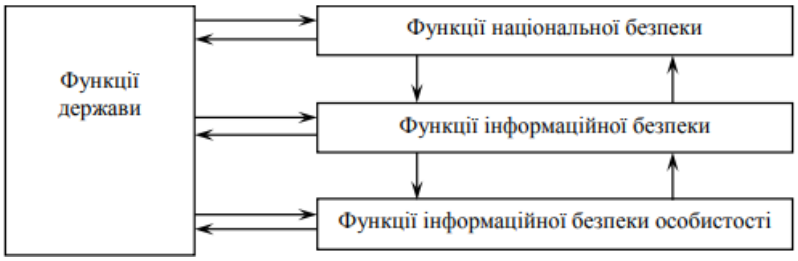

Рисунок 1.1. – Взаємозв'язок між видами інформаційної безпеки

1.2 Поняття інформаційної безпеки особистості

Безпека людини — стан, при якому навколищні фактори не призводять до погіршення функціонування організму чи його розвитку, не впливають на свідомость і психіку людини загалом.

Особистість- це передумова і продукт існування суспільства та держави. У процесі стрімкого розвитку інформаційного простору людина стає все більше інформаційно «відкритою». Так будь-яка інформація про особистість може бути використана іншими особами. При наявності необхідних засобів та бажання, можна легко отримати доступ до інформації майже про кожну людину. Лише невелика частина населення має здатність запобігати небажаному доступу до власної інформації. Тому багато людей досі залишаються інформаційно незахищеними.

Інформаційна безпека особистості — здатність та готовність захищати себе та свій внутрішній світ від загроз, пов'язаних з обмеженням прав та свобод кожної людини в інформаційній сфері.

Інформаційну безпеку особистості можна класифікувати наступним чином:

- інформаційно-технічна – захист інформації та області, що підтримується, від шкідливих впливів різного характеру, що несе загрозу заподіяння шкоди володільцям інформаціїї, її користувачам або середовищу. В цьому випадку мається на увазі саме безпека інформації особистості.
- інформаційно-психологічна - це захищеность людської психіки від негативних впливів інформаційного характеру, що здійснюються впровадженням деструктивної інформації у людську свідомість чи підсвідомість.

В більшості випадків реалізація захисту інформаційної безпеки особистості залежить від належної підготовки особистості та її можливості протидіяти інформаційним загрозам, а також від державного забезпечення інформаційних потреб людини, розвитку інформаційного середовища та рівня його захищеності.

Інформаційна безпека особистості має наступні функції:

- забезпечення придатних умов для життєдіяльності;
- проведення аналізу загроз власної безпеки;
- безпека соціальної комунікації з іншими особами;
- формування світогляду та правосвідомості;
- підвищення рівня знань та навичок, що необхідні для роботи з інформацією;
- формування свідомого уявлення про органи державної та місцевої влади, які є суб'єктами державної національної безпеки.

Відповідно до Доктрини інформаційної безпеки України, пріоритетними інтересами особи в інформаційній сфері України визначаються наступні:

- забезпечення конституційних прав і свобод людини для цієї сфери;
- захист персональних даних від неправомірного доступу та модифікації, а також захист даних під час обробки чи використанні;
- захист від негативних інформаційних впливів психологічного характеру.

1.3 Аналіз нормативно-правової бази інформаційної безпеки особистості

Стрімкий технологічний розвиток світу не тільки сприяє вирішенню великої кількості проблем його еволюції людської цивілізації, але й призводить до появи нових ризиків і загроз інформаційного простору, так як інформація може бути не тільки корисною, а й небезпечною для особистості та держави в цілому. Проблему правового забезпечення у сфері інформаційної безпеки можна віднести до однієї з найбільш пріоритетних, адже розвиток державності у сучасному світі неможливий без взаємодії з глобальним інформаційним середовищем.

Основоположні інформаційні права і свободи людини тісно пов'язуються та описуються іншими правами і свободами, що визначені Конституцією. .

На конституційному рівні описано більше 20 норм права з визначенням інформаційні права та свободи, або ж стосуються інформаційної сфери:

- свобода від цензури (стаття №15).
- право на збереження таємниці листування, телефонних розмов, тощо (стаття № 31);
- право на приватність та невтручання у особисте та сімейне життя (стаття №32);
- право на вільне волевиявлення (стаття № 34);
- право інтелектуальної власності (стаття № 41)
- право можливість вірного розвитку (стаття № 23);
- право на повагу до гідності (стаття № 28);
- право на можливість робити зібрання (стаття № 39);
- свобода власної творчості (стаття № 54) та інші.

Права і свободи людини у інформаційній сфері складають достатньо розширену систему, адже національне законодавче забезпечення України складається зі великого масиву правових актів, які мають вплив на регуляцію інформаційних суспільних відносин.

Проаналізувавши деякі документи, можна сказати, що основними нормативними документами, у яких описані основоположні визначення, що стосуються забезпечення національної інформаційної безпеки, є такі конституційні закони:

- «Про інформацію»;
- «Про Національну програму інформатизації»;
- «Про доступ до публічної інформації»;
- «Про захист інформації в інформаційно-телекомунікаційних системах»;
- «Про захист суспільної моралі»;
- «Про захист персональних даних».

Наведені вище акти описують регуляцію взаємовідносин між суб’єктами інформаційної безпеки на різних рівнях, їх права, обов’язки та відповідальність . На основі аналізу зазначених документів можна засвідчити про наявність великої

кількості прогалин. Так, нині в законодавстві навіть немає чіткого визначення поняття «інформаційна безпека», навіть попри його регулярне використання.

Проведемо короткий аналіз цих документі та зазначимо основні положення, що стосуються інформаційної безпеки особистості.

1) Закон України «Про інформацію».

Згідно положень, визначених у законі, основними принципами інформаційних взаємовідносин є:

- гарантія інформаційного права;
- забезпечення безперешкодного доступу до публічної інформації,, свободи при обміні інформацією;
- достовірність і повнота інформації;
- можливість вільно виражати свої переконання та погляди;
- правомірне використання можливостей поширення, зберігання та захисту інформації;
- захист особи від втручання в особисте життя.

2) Закон «Про Національну програму інформатизації».

У ньому описані комплекні завдання для проекту інформатизації, що спрямовані на реалізацію політики держави та її пріоритетів інформаційної інфраструктури. Також цим законом координуються державні органи, органи місцевого самоврядування та організації, установи чи підприємства у сфері інформатизації.

3) Закон України «Про доступ до публічної інформації».

Цей акт описує права людини на таку і інформацію, а також права людини як суб’єкта такої інформації.

У статті 10 цього закону визначені основні принципи щодо публічної інформації конкретної особистості.

Таким чином, особа має наступні права:

- знати мету та цілі збору інформації про неї, та методи подальшого застосування цих даних до початку їх використання;

- мати доступ до інформації, яка про неї збирається, зберігається та використовується;

- коригувати неточну, неповну чи застарілу інформацію про себе, а також вимагати знищення інформації про себе, яка збирається чи використовується з порушенням чинного законодавства;

- на доступ до інформації про іншу особу, якщо від цього залежить реалізація чих захист її прав або інтересів;

- відшкодування збитків та завданої шкоди через неправомірне використання інформації про неї.

Також визначено, що публічна інформації про особу має бути максимально обмеженою і використана лише конкретною метою, яка визначена законом.

Особи, які є володільцями інформації, що стосується інших людей мають забезпечити наступне:

- безкоштовне надання інформації про особу цій особі за її вимогою;
- використання інформації лише з визначеною метою та способами;
- забезпечувати захист інформації від несанкціонованого доступу;
- коригування неточної та застарілої інформації за власним бажанням чи за вимоги осіб, що є суб'єктами цієї інформації.

Збереження та поширення даних має закінчуватися після досягнення мети збору і поширення. При відмові особі надати доступ до інформації про неї, або приховане використання таких даних, особо може подати скаргу з метою відстоювання своїх інтересів.

4) Закон України «Про захист суспільної моралі».

Цей документ містить визначення забороненої інформації та принципи обмеження такої інформації.

Згідно цього закону, заборонено створення та поширення такої інформації:

- пропаганда війни, розпалення національної чи релігійної ворожнечі, підбурювання державного перевороту;
- пропагування ідеологій фашизму та неофашизму;
- приниження особистості через національність;

- пропаганда бузувірства, блюзнірства, та неповаги святинь;
- приниження особистисто та знущання над нею;
- пропаганда невігластва;
- пропаганда наркотиків, інших токсичних речовин і шкідливих звичок.

Державна політика у сфері захисту суспільної моралі визначається створенням спеціальних на правовому, економічному та організаційному рівні умов, необхідних для сприяння реалізаціїї прав людини у інформаційному просторі, для захисту населення від фізичних, інтелектуальних та психологічних загроз.

Основні напрями регулювання інформаційного обігу на державному рівні:

- комплексна система забезпечення захисту моральних принципів і засад у культурній, освітній та інформаційній діяльності;
- запобігання поширенню забороненої інформації і пропаганди інформаційними ресурсами та засобами масової інформації;
- експертна оцінка друкованої інформації та електронної інформації, спеціально розробленими механізмами і методиками;
- розвиток сфери національної культури та популяризація літератури, культури та мистецтва;
- унеможливлювання використання неліцензійної продукції на рівні національного телебачення;
- контроль обігу загрозливої для суспільної моралі продукції;
- заключення міжнародних договорів для захисту суспільної моралі.

5) Закон України «Про захист персональних даних».

В цьому документі містяться основні визначення щодо використання та поширення персональних даних.

Згідно до статті 1, цим законом регулюються правові відносини у сфері захисту і обробки даних. Він був створений для захисту основних прав і свобод людини, особливо право на захист від втручання в особисте життя через.

Цей Закон стосується загалом діяльності з обробки персональних даних шляхом використання автоматизованих засобів, а також обробки персональних даних, призначених для використання картотеки. У стаття 6 сказано, що обробка

персональних даних має здійснюватися відкрито і прозоро. Засоби, що застосовуються для обробки, мають відповідати цілям. Такі цілі визначаються чинним законодавством та за згодою особи. Обробка конфіденційної інформації про особу забороняється цим законом. Закон забороняє обробку персональних даних, які стосуються расового чи етнічного походження, політичних та релігійних переконань, членства в організаціях, про здоров'я, статеве життя, а також біометричної чи генетичної інформації.

1.4 Постановка завдання

1) Аналіз теоретичних аспектів інформаційної безпеки особистості.

В цьому завданні необхідно теоретичний матеріал щодо інформаційної безпеки загалом, та інформаційної безпеки особистості.

2) Аналіз нормативно-правових актів в законодавстві України, які забезпечують інформаційну безпеки особистості.

Необхідно вивчити основоположні акти законодавчого рівня з інформаційної безпеки та визначити аспекти, що стосуються, регулюють та забезпечують інформаційну безпеку особистості.

3) Проаналізувати можливі шляхи та види загроз інформаційній безпеці особистості.

Для виконання цього завдання потрібно дослідити варіанти можливих загроз та ризиків особистості в інформаційному середовищі.

4) Побудувати модель порушника інформаційної безпеки особистості.

На основі аналізу загроз та ризиків створити модель порушника безпеки.

5) Розробити рекомендації для забезпечення захисту інформаційної безпеки особистості.

За принципом моделі порушника, розробка методичних рекомендацій щодо забезпечення інформаційної безпеки особистості, які призначені для самої особистості.

Висновки до розділу 1

В першу чергу було проведений аналіз теоретичних аспектів інформаційної безпеки в цілому та інформаційної безпеки безпосередньо особистості. На даний момент, питання інформаційної безпеки особистості немає чіткого визначення та розглядається лише дотично до інших проблем інформаційної безпеки.

Також було визначено основні закони, які в тій чи іншій мірі розкривають поняття інформаційної безпеки особистості у правовому полі. Загалом аналіз різних документів свідчить про наявність істотних прогалин. Кількість законів в інформаційній сфері не переростає в якість.

Недоліками законодавства у інформаційній сфері є відмінність визначених норм у численних документах з різною юридичною силою, неузгодженість більшості чинних актів між собою; а також наявність великого масиву норм, які не визначають шляхи реалізації.

Тому в нашій країні спостерігається низький рівень реалізації норм права, що забезпечують регулювання інформаційної безпеки; а також наявність численних відсильних норм права, абстрактних і суб’єктивних понять, які потребують офіційного тлумачення та визначення. Більш того, на законодавчому рівні спостерігається відсутність навіть базових визначень, що стосуються питання інформаційної безпеки.

РОЗДІЛ 2. МОДЕЛЬ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ

Питання інформаційної безпеки особистості включає в себе кілька аспектів: технічно-інформаційний та інформаційно-психологічний.

Технічний аспект пов'язується із безпосередньо захистом інформації та ресурсів інформаційного середовища, тобто це захист джерел доступу, збереження та передавання інформації, захист інформаційних ресурсів за рівнем доступу. Соціально-психологічний аспект пов'язується із захистом психологічної безпеки особистості від шкідливих впливів інформаційного простору.

2.1 Модель інформаційно-психологічного впливу на безпеку особистості

Такий вплив розглядається як можливості впливу на свідомому та підсвідомому рівні на особистість та населення з метою зміни їхньої поведінки та світосприйняття.

Критеріями безпеки від психологічних впливів є ресурси особистості. Ресурсами особистості називають певні психологічні опори, які допомагають людині у забезпеченні своїх основних потреб.

Рівень цих ресурсів залежить від наступних факторів:

- рівень сформованості уявлення про інформаційно-психологічну безпеку (наявність достатньої інформаційної бази сприяє при формуванні механізмів захисту від інформаційних загроз);
- критичність мислення (вміння аналізувати різну інформацію для визначення ступеня її логічності та ефективності при застосуванні в конкретній ситуації);
- психологічна стійкість.

Виходячи з вищезазначених критеріїв, можна зобразити інформаційно-психологічну безпеку особистості у вигляді моделі, де відображаються джерела загроз, особливості інформації та вплив на різні рівні ресурсів особистості.

Модель наведена нижче на рисунку 2.1.

Рисунок 2.1-Модель інформаційно-психологічної безпеки особистості

На основі аналізу цієї моделі можна зробити такі висновки:

1) Існують такі інформаційні ризики, які мають вплив на психіку людини на різних рівнях, різними способами і засобами, що роблять можливим маніпуляцію свідомістю особи та призводить до хибного сприйняття нею дійсності.

2) Інформація взаємопов’язана із суспільством, різними групами та особистістю.

3) В першу чергу, інформаційно-психологічна безпека особистості залежить від ресурсів особистості, які, в свою чергу залежать від розвитку цієї особистості.

4) Визначено три рівні ресурсів особистості щодо забезпечення інформаційно-психологічної безпеки. Характеристика цих рівнів наведена на рисунку 2.1.

Класифікація можливих психологічних впливів:

- переконання – аргументований вплив на свідомість іншої людини з метою зміни їх суджень, відношення до чогось, намірів чи рішень;
- самопросування;
- маніпуляція – прихований вплив на систему світобачення людини;
- заклики до наслідування інших людей;
- примус;
- деструктивна критика – агресивна і зневажлива оцінка іншої особи;
- ігнорування – зневажливе ставлення до уваги з боку іншої людини, що підкреслює її неприйняття у суспільстві людини, а також може бути тактичною формою примусу;
- передача емоційного стану;
- навіювання –створення схильності особистості до певних дій шляхом підсвідомого впливу.

Наслідки інформаційних впливів виявляються у наступних ефектах:

1)Когнітивні ефекти проявляються через зміну рівня інформованості, розширенні обсягу знань; появі нових когнітивних зв'язків та способів сприйняття дійсності.

2)Емоційні ефекти виражаються зміною емоційного стану та почуттів людини, зміною емоційно-психологічного фону людського існування, появою різкого імпульсу до активних роздумів, переробки чи трансформації інформації.

3)Ціннісні ефекти виражаються формуванням нових або зміною наявних інтересів, поглядів та ставлення до самого себе або інших.

4)Фізіологічні ефекти визначається змінами фізичного стану людини.

5)Поведінкові ефекти виражаються через дії та вчинки людини.

Таким чином джерела загроз психологічній безпеці особистості в інформаційному середовищі включають в себе можливість впливів, можливість

використання фізичного середовища, а не лише інформаційного, та стан об’єкту на який здійснюється вплив.

2.1 Модель порушника для інформаційно-технічного аспекту

2.2.1 Загрози фізичного середовища

Нижче на рисунку 2.2 схематично представлене узагальнене зображення фізичного інформаційного середовища особистості. Загрози фізичного середовища – це можливі небезпеки для кожної його складової.

Рисунок 2.2 -. Фізичне інформаційне середовище особистості

Загрози при використанні персонального комп’ютера

Проникнення в операційне середовище комп'ютера дає зловмиснику можливість несанкціонованого доступу:

- до базової системи введення/виведення (BIOS), інформації про систему та її команд. Завдяки цьому порушник має змогу здійснювати керування завантаженням операційної системи та отримувати права доступу довіреного користувача;

- до середовища функціонування операційної системи технічного засобу з можливістю запуску програмних компонентів цієї операційної системи або спеціально завантажених засобів;
- до середовища виконання прикладних програм;
- безпосередньо до інформації користувача, що знаходиться на пристрої.

За умовами реалізації загрози отримання фізичного доступу до персонального комп'ютера можна класифікувати наступним чином:

1) Реалізація загроз відбувається при завантаженні операційної системи пристрою. Такі атаки проводяться для того, щоб перехопити парольні дані, змінити налаштування BIOS, налаштувати пристрій зі встановленням контролю над процесом завантаження системи.

2) Загрози, які реалізуються після завантаження пристрою. А саме операційної системи комп'ютера. Такі атаки зазвичай використовують з метою отримання несанкціонованого проникнення до даних на пристрої. Крім стандартних програм операційної системи, зловмисники можуть використовувати програмні засоби, що були розроблені спеціально для таких атаки.

Завдяки таким розробкам, зловмисники отримали можливість виконувати наступні задачі:

- перегляд та модифікація реєстру;
- текстовий пошук серед усіх файлів за допомогою ключових слів та копіювання знайденої інформації;
- перегляд та копіювання записів з баз даних;
- швидкий перегляд графічних файлів, їх редагування чи копіювання;
- реконфігурація програмних засобів.

3) Реалізація загроз визначається фактом запуску будь-якої з прикладних програм. В основному, це загрози впровадження шкідливих програм.

Отримання несанкціонованого доступу до пристрою можливе через:

- робочу станцію користувача: термінал, клавіатуру або засоби відображення інформації;
- засоби документування інформації;

- засоби завантаження програмного забезпечення;
- внутрішній монтаж персональних комп'ютерів;

Загрози використання мобільних пристроїв

Сучасний світ неможливо уявити без використання мобільного пристрою. Бездротовий телефон давно перестав бути лише засобом забезпечення голосового зв’язку. Зараз смартфон – це цілий інформаційних світ у вашій долоні. Через це їх використання стало невід’ємною складової життєдіяльності людини і суспільства в цілому. Використання цього девайсу значно спрощує наше існування та робить комфортнішими майже усі сфери життя. Однак, таке використання пристрою, призвело до того, що, в разі отримання доступу до мобільного телефону особи, уся інформація з пристрою також стає доступною і може бути використанна проти неї самої.

Саме через це мобільні пристрої вже довгий час є однією з найпривабливіших цілей для зловмисників. Перелік можливих загроз для мобільних пристроїв на даний момент вже є достатньо великим і продовжує постійно поповнюватись.

Загрози безпеці мобільних пристроїв можна умовно поділити: шкідливі впливи на роботу пристрою та атаки пристроїв.

Найбільш поширеним є використання наступних впливів:

- використання технологій Bluetooth та MMS для поширення інформації різного характеру;
- зараження локальних файлів;
- завантаження невідомих файлів з глобальної мережі;
- можливість дистанційного керування пристроєм;
- зміна відображення програм у системі девайсу;
- некоректне використання шрифтів та застосунків;
- знешкодження систем захисту та антивірусів;
- створення завад для роботи носіїв інформації;
- викрадення інформації та порушення її цілісності;
- відправка SMS та здійснення дзвінків на платні номери.

Найпопулярніші атаки на мобільні пристрої:

1) Програми-вимагачі.

Це спеціальні програми, що блокують роботу пристрою з метою отримання викупу. В цьому випадку власник пристрою може повернути контроль свого девайсу після здійснення виплати викупу.

Однією з найбільш небезпечних програм у цій категорії є програма під назвою «DoubleLocker».Це – перший мобільний шифратор, який паралельно використовує службу спеціальних можливостей. Це означає, що програма здатна не тільки зашифровувати дані майбутньої жертви, а також здатна змінювати коди доступу до девайсу. Таким чином власник телефону не зможе навіть розблокувати свій пристрій.

2) Ботнети.

Це мережа пристроїв, інфікованих шкідливим програмним забезпеченням. Така мережа знаходяться під контролем зловмисників і дає їх можливість ініціювати DDoS-атаку на будь-який ресурс, чи почати масове поширення спам-листів.

3) Шкідливі програми.

Такі програми зазвичай здаються безпечними, тому користувачі без остраху їх встановлюють та використовують відповідно до, заявленого «розробником», функціоналу програми. Насправді, це добре замасковані програми, які лише виглядають легітимними, оскільки містять вбудований шкідливий код. Таким чином людина нібито встановлює відеоплеєр, а отримує бомбу заповільненої дії. Шкідливу програму розміщують разом зі справжніми застосунками на спеціальних для цього платформах. Програми зі шкідливим кодом можуть бути поширені навіть на офіційних магазинах додатків відомих компаній. Наприклад, в офіційному магазині Play Store Google, одного разу фахівці виявили понад 300 програм зі шкідливим кодом. Не завжди рятують і заходи безпеки від Google та Apple для своїх магазинів. Так, у Google Play, було виявлено на шпигунську програму яка, під видом месенджера, виконувала збір приватних даних, записи дзвінків та особистих повідомлень користувачів.

4) Атаки через безконтактні платежі.

NFC (Near Field Communication) – це технологія бездротового зв’язку, яка дозволяє обмінюватися даними на малих відстанях. В мобільних пристроях використовується для забезпечення технології безконтактної оплати. Ця функція є досить корисною та зручною для користувачів. Хоча, NFC вважається захищеною технологією, не варто недооцінювати можливі загрози її використання. Під час обміну інформації між смартфоном та пристроєм зчитування використовується стійкий тип шифрування, який забезпечує необхідний рівень захисту платіжних даних. Але частина інформації під час передачі таки залишається відкритою і може бути перехоплена. Невелика відстань при передачі обміну підвищує захист технології. Але при використанні спеціальних пристроїв зчитування у зоні дії технології під час передачі зловмисники можуть перехопити перехопити деякі і отримати доступ до даних, в тому числі і платіжних.

Загрози Інтернету-речей

Пристрої Інтернету речей або іншими словами система пристроїв «розумного дому» також є складовою безпеки фізичного середовища.

Можна виділити основні загрози, які використовують порушники, націлені на такі атаки:

1) Несанкціонований доступ до системного контролеру.

Контро́лер — спеціальний компонент системи, який виконує керування підключених зовнішніх пристроїв, а саме. Таким чином, Інтернет-речей-це система розумних девайсів, поєднаних єдиним пунктом управління. Такий контролер приваблює зловмисників. Реалізація успішної атаки і отримання несанкціонованого доступу може мати жахливі наслідки. Якщо зловмик проникне до цього контролеру, маючи права доступу адміністратора, то система в цілому стане небезпечною. Проникнення може бути спричинене некоректним керуванням паролями і ключами, або підключенням до мережі неавторизованих пристроїв.

2) Легка доступність до середовища домашньої мережі.

Через те, що система «розумного дому» підключена до глобальної мережі, зловмисники можуть атакувати дистанційно, через мережеві інтерфейси управління, або через встановлення шкідливого програмного забезпечення.

3) Можливість фізичного доступу до системи.

Це стосується не лише зв'язку по лініях електропередач, а й бездротових технологій. Зловмисник може проникнути ззовні до фізичної мережі та отримати доступ до усіх пристроїв.

4) Обмеженість системних ресурсів.

5) Неоднорідність систем, які вбудовані у пристрої.

Виробники пристроїв «розумного дому» використовують різні мережеві стандарти та можливості оновлення програмних застосунків. Часто пристрої взагалі не мають документації до операційної системи чи встановлених механізмів безпеки.

6) Фіксована прошивка.

Регулярне оновлення програмного забезпечення забезпечує виправлення вразливостей розробником. Фіксована прошивка унеможливлює оновлення, що робить пристрої більш вразливими.

7) Повільне впровадження стандартів.

Досі не розроблено єдиной стандарт безпеки для таких систем. Це стало причиною того, що, більшість пристроїв «розумного будинку» не мають достатньої кількості реалізованих підодів до безпеки.

Загрози Wi-Fi мережі

1) Зміна налаштувань DNS-сервера.

Зловмисник здійснює зміну налаштувань DNS-серверу, відповідно до цілей своїх отак. Наприклад, під час виконання запиту у браузері, жертва може бути перенаправлена на ресурс, який зловмисник задає у налаштуваннях. Це може призвести до перехоплення трафіку усієї мережі чи до зараження пристроїв, які цю мережу використовують.

2) Перехоплення особистої інформації

В цьому випадку використовується атака типу «людина посередині» (man-in-the-middle, MitM). За замовчуванням, мережевий веб-трафік одразу надсилається до роутера. Реалізація такої акаки дозволяє зловмиснику стати проміжним пунктом при передачі даних. Таким чином, весь трафік мережі спочатку відправляється

зловмиснику, і вже від зловмисника до Wi-Fi роутера. Таке перехоплення є непомітним з боку самого роутера.

3) Виконання дій від імені мережі..

Усі дії користувачів в мережі залишають сліди і можуть бути виявленими та ідентифікованими. За злам сайтів, DDOS-атак чи поширення забороненої інформації взагалі передбачене кримінальне правопорушення. Зловмисник може приховати свою причасність до таких дій шляхом використання чужих Wi-Fi мереж. Він проникає безпосередньо до мережі і тоді вся діяльність буде виконуватися вже від імені власника цієї мережі.

2.2.2 Загрози цифрового середовища

На рисунку 2.3 схематично зображені загрози можливі у цифровому середовищі особистості

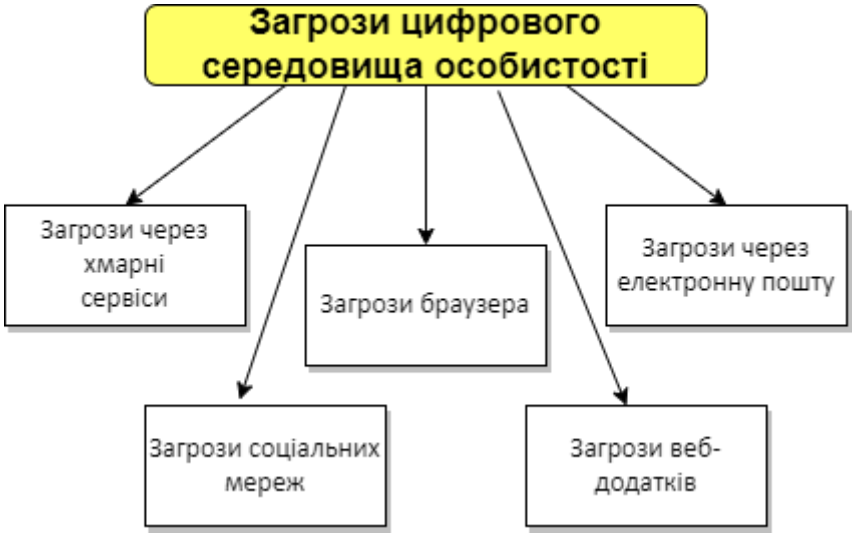

Рисунок 2.3 - Загрози цифрового середовища особистості

Загрози при використанні хмарних технологій

1) Загрози витоку інформації.

Хмарні загрози є майже ідентичними традиційним фізичним. Загрози витоку конфіденційної інформації є важливою проблемою і для хмарної інфрастуктури.

Зловмисники все частіше атакують хостинг-провайдерів хмарних сервісів. Це може призвести до серйозної небезпеки для даних, які зберігаються у хмарі.

2) Зламування інтерфейсів і API.

Використання графічного інфтерфейсу значно спрощує керування ресурсами і налаштуваннями для користувача.

Однак може становити становити загрозу для безпеки усієї хмари. Тому до його вибору необхідно підходити досить серйозно. Оскільки, безпека усієї інфрастуктури безпосередньо залежить від якості опрацьовання механізмів керування доступом до графічного інферфейсу. Таким чином від вибору від того, наскільки якісно опрацьовані механізми контролю доступу, може безпосередньо залежати безпека вашої інфраструктури. Проблемою використання користувацьких інтерфейсів є наявність прогалин зі сторони безпеки. Зловмисники в свою чергу виявляють і використовують ці прогалини.

3) Вразливість систем.

У наш час популярність використання публічніх послуг стрімко зростає. Публічні послуги – це можливість одночасного використання якоїсь послуги декількома людьми. Але варто зауважити, що зі збільшенням користувачів, збільшує вразливість системи до певних небезпек.

4) Обхід автентифікації.

Механізми аутентифікації користувачів мають бути реалізовані належним чином, оскільки зловмистини часто реалізують свої атаки саме через недоліки цих механізмів та механізмів розмежування правами доступу.

5) Кібератаки.

6) Крадіжка облікових записів.

Фішинг атаки залишаються актуальними і при використанні хмарної інфраструктури. Небезпека для хмарної інфраструктури може становити і фішинг. Зловмисники використовують методи соціальної інженерії, а саме викрадення даних облікового запису через шкідливі сайти, експлойти та маніпуляції з транзакціями чи зміною даних.

7) Недостатня поінформованість.

Користувачі мають розуміти принципи розгортання програм у хмарномо середовищі, та дотримуватися їх на практиці. Це сильно зменшує ризик виникнення операційних проблем і проблем безпеки через некоректне використання клієнтами хмари.

8) DDoS-атаки.

Як правило, такі атаки націлюються на вразливісті баз даних та серверів хмарного середовища. Їх реалізація спричиняє перезавантаження системи та навіть унеможливлює її використання.

9) Використання спільних технологій.

Такі ризики обумовлюються появою вразливостей на одному з рівнів хмарної інфраструктури та їх поширення і на навколишні рівні. Тож може здійснюватися вплив вже на всю інфраструктуру в цілому.

10) Зловживання cloud-сервісами.

Використання будь-яких послуг в інформаційній сфері має буди свідомим та цільовим. Це стосується і хмарних технологій. Користувач має усвідомлювати основні переваги та недоліки, а також розуміти свою мету переходу та використання цих можливостей.

Загрози використання браузера

Типи можливих атак на особистість під час використання браузера:

1) Підроблені розширення.

Плагіни та розширення у браузері призначені для зручності користувачів та збільшення ефективності використання самих браузерів людиною. Існує багато дійсно корисних розширень, наприклад організатори вкладок, менеджери паролів та менеджери керування завантаженнями тощо. Зловмисники використовують підроблені розширення з метою заволодіння інформацією. Зазвичай ці додатки розміщуються на незахищених сайтах. Таким способом можливе перехоплення інформації з браузеру, паролів та інших особистіх даних.

2) Перехоплення сеансу.

При реєстрації у будь-якому онлайн-сервісі, призначається унікальний ідентифікатор сеансу. Пристрій здійснює обмін цього ідентифікатору для перевірки

сеансу. Якщо цей ідентифікатор автентифікації зашифрований неправильно, виникає серйозна проблема безпеки, через можливе перехоплення даних після такої перевірки. Далі зловмисник виконує безпосередньо саме захоплення сеансу. Після чого дії порушника ідентифікуються як дії законного користувача. При підключенні до незахищеної мережі Wi-Fi, браузер стає особливо вразливим до таких атак.

3) SQL-ін'єкція.

Команди SQL надсилаються зловмисником на веб-сервер з метою отримання доспуту до інформаціїї, її викрадення чи модифікації. Порушники впроваджують шкідливий код у браузер через пошкодження різних веб-форм або файли cookie. Це призводить до того, що завантаження такої веб-сторінки ініціює виконання коду. В залежності від самого коду, можливе викрадення особистої інформації, платіжних даних, паролів тощо. В цьому випадку атака вплинає на сам веб-сайт, або сервер, до якого ми намагаємося отримати доступ з браузера.

4) Атаки типу Man in the Brauzer.

Цей тип атаки реалізуєть яка стоїть між жертвою та сервером, до якого вони намагаються отримати доступ. Це те, Такі атаки типу «людина посередині» або, більш конкретно в даному випадку, «людина у браузері» (Man in the Brauzer). Зловмисники виконують перехоплення усього трафіку браузера, який надсилається та отримується при вході на веб-сторінку, вході в систему тощо. Окрім викрадення даних, також можлива модифікація самого трафіку. Це означає, що зловмисник може змінити інформацію веб-сайту і призвести до використання фальшивої веб-сторінки.

5) Використання вразливостей браузера.

Зловмисники використовують вразливості і помилки самих браузерів та встановлених розширень.

Загрози веб-застосунків

Веб-застосунок (Web Application) — це програмне забезпечення, доступ до якого отримується шляхом завантаження веб-сторінки, та у якому браузер виконує роль клієнта, а сервер — веб-серверу.

Загрози інформаційної безпеки Web-застосунків можна розділити на кілька видів:

1) Міжсайтовий скриптинг- використання шкідливого JavaScript–коду через його впроваження у код веб-застосуноку. Виконання коду відбувається при завантаженні сторінки браузера. Такі атаки в основному націлені на дані автентифікації входу

2) SQL-ін’єкція – впровадження шкідливого SQL-коду в тіло HTTP-запиту.

3) CRLF-атака – модифікації HTTP-заголовків запиту.

Поділяється на:

а) CRLF-ін’єкцію – формування «шкідливих» URL через використання ASCII;

б) Розшарування HTTP-запиту. Дозволяє сформувати URL, для підміни відповіді сервера, та ініцації внутрішніх помилок.

4) XXE (XML eXternal Entity)-атаки.

5) CSRF (Cross Site Request Forgery) – міжсайтова підробка запитів дозволяє використання автентифікаційних даних відповідної особи (cookies) і проводити різні шкідливі операції від її імені.

6) DDoS-атака – виконання зовнішніх запитів з різним трафіком, яке призводить до переповнення пам’яті та відмови в обслуговуванні системи. Під час такої відмови можна отримати доступ до ресурсу і root-прав.

Загрози соціальних мережах

Зазвичай загрози орієнтовані на особисту інформацію користувача та його друзів.

1) Clickjacking або “Викрадення кліку”.

Це певна шахрайська техніка, яка змушує користувача робити «клік» , тобото натискати на те, що хоче зловмисник, а не сам користувач. Завдяки цій техніці, порушник має можливість маніпуляції користувачем для поширення спам-публікацій. Також зловмисник отримує можливість керування пристроєм, наприклад увімкненням веб-камери чи мікрофону.

2) Деанонімізація.

Більшість соціальних мереж мають додаткові функції, які допомагають захистити анонімність людини і її конфіденційність. Для здійснення атак, що направлені на деанонімізацію особистості, зловмисники відстежують файли cookie, мережеві топології, інформацію з відкритих джерел, наприклад про членство у користувацьких групах. Всі ці дії мають на меті поставити під питання анонімність користувача, та розкрити його особистість.

3) Розпізнавання обличчя.

Соціальні мережі використовуються у різних цілях. Однією з таких цілей є публікація власних фото для того, щоб поділитися ними зі своїми друзями. Це призвело до того, що кожного дня завантажуються мільйони особистих фото до мережі. На основі цих знімків може бути створена біометричні база даних, яка ідентифікує особистість користувача по фотографії без його на це дозволу.

4) Fake-профілі.

Це створення підробних профілів з метою імітаціїї поведінки людини у соціальних мережах. Вони можуть бути автоматичними та напівавтоматичними, або ботами, та мають на меті збір персональних даних користувачів.

5) Атаки клонування.

Техніка, за допомогою зловмисники виконують дублювання присутності якогось користувача в соціальній мережі. Це робиться для того, щоб сформувати довірчі відносини з друзями клонованого користувача. Користуючись такою довірою, зловмисник збирає особисту інформацію від друзів свого клону, та займається онлайн-шахрайством.

6) Атаки логічного висновку.

Цей тип атак для соціальної мережі використовується для передбачення конфіденційної інформації користувачів. Найчастіше це стосується особистої інформації людини, яка не розголошуватися без її бажання. Наприклад, релігійна приналежність, сексуальна орієнтація. Для реалізації атаки такого типу використовуються інтелектуальні методи аналізу інформації для поєднання загальнодоступних даних та інформації з особистої сторінки користувача мережі та його друзів.

7) Виявлення геопозиції людини.

З появою смартфонів значно збільшилось бажання людини поширювати приватну та чутливу інформацію у соціальних мережах. Особливо небезпечним може бути інформація про геопозицію. Користувачі інколи беззастережно поширюють дані про власне поточне місцезнаходження , або їх локацію у майбутньому. Така інформація може бути використана з різними цілями, що становить для людини конкретну небезпеку.

8) Шкідливі програми для соціальних мереж.

Socware – це збірна назва від поняття «social malware» та означає соціальні шкідливі програми. Вони розроблені спеціально для соціальних мереж з метою публікації фальшивих та часто шкідливих дописів та повідомлень нібито від друзів користувача соціального сервісу. Для прикладу, через використання socware можна заохотити людину встановити застосунок зі шкідливим кодом або відвідати небезпечний веб сайт .

Загрози при застосуванні електронної пошти

Різновиди атак через використання електронної пошти:

- віруси;
- спам різного класу – від комерційних розсилок до повідомлень про виграші в несуществующих лотереях;
- управління інформацією з фішингових адресів, які імітують реальні. Їх відвідування призводить до використання конфіденційної інформації. Найчастіше такі листи приходять нібито від імені банків і мають на меті отримання платіжних даних користувачів;
- листи з неправдивою інформацією, розраховане отримання від користувачів конфіденційних даних;
- цільові спроби отримання доступу до інших сервісів.

Висновки до розділу 2

Інформаційна безпека особистості складається технічно-інформаційної та інформаційно-психологічної безпеки людини. В цьому розділі наведено опис кожної складової. На основі аналізу технічно-інформаційної складової було проведено класифікацію можливих загроз безпеці особистості та побудовано модель порушника на основі визначеної класифікації.

Модель порушника складається з загроз для фізичного та цифрового середовищ. Загрози для кожного середовища класифікуються відповідно до шляхів їх реалізації

Це надає можливість створення рекомендацій для захисту інформаційної безпеки особистості у послідовному та структурованому вигляді.

РОЗДІЛ 3. РЕКОМЕНДАЦІЇ ЩОДО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИСТОСТІ

3.1 Захист фізичного середовища особистості

Захист персональних комп’ютерів

Забезпечення захисту даних персонального комп’ютера реалізується багатьма методами та засобами, що відрізняються кінцевою метою чи технічним втіленням. Умовно такі засоби можна класифікувати як апаратні, механічні та програмні.

1) Механічні засоби представлені у вигляді різноманітних кришок та чохлів з замками, клейких пластин, використанні сигналізації. Використання кришок та чохлів дає можливість замикання самого пристрою, дисководу, мережевого вимикача. За допомогою клейких пластин можна прикріпити девайс до якоїсь поверхні, щоб запобігти його викраденню. А, використовуючи сигналізацію помешкання, власник буде завжди інформований про спроби несанкціонованого доступу до нього.

2) Апаратні засоби- це спеціальні електронні модулі, що виконують підключення до комп’ютерного системного каналу або портів введення/виведення. Вони використовуються для обміну кодовими послідовностями для захисту програм

3)Програмні засоби захисту мають найбільшу різноманітність. До них належать програми шифрації даних по заданому користувачем ключу; адміністрування дискового простору, з метою розмежування доступу користувачів; програми, які обмежують встановлення іншого програмного забезпечення, за конкретно визначеними критеріями; а також використання спеціальних захисних програмних оболонок для програм, що потребують захисту.

Загалом можна виділити такі стандартні захисні засоби для персональних комп’ютерів:

- засоби захисту обчислювальних ресурсів, що використовують парольну ідентифікацію й обмежують доступ несанкціонованого користувача;
- застосування різноманітних методів шифрування, що не залежать від контексту інформації;
- захист від комп'ютерних вірусів;
- створення архівів та резервне копіювання даних.

Захист мобільних пристроїв від несанкціонованого доступу:

Для захисту мобільних пристроїв користувачу необхідно виконувати такі прості дії:

- регулярно оновлювати операційну систему та інше програмне забезпечення. Це дозволяє зменшити кількість загроз для пристрою, оскільки розробники виправляють вразливості своїх розробок у нових версіях програмного забезпечення;
- використання складних та унікальних паролів для захисту пристрою, а також двофакторної аутентифікації для забезпечення захисту акаунтів мобільного банку, електронної поштової скриньки та соц.мереж;
- завантаження додатків перевірених розробників;
- шифрування даних на пристрої;
- бездротове резервне копіювання даних. Варіанти резервного копіювання залежать від операційної системи конкретного пристрою. Створивши резервну копію для вашого смартфона або планшета, можна легко відновити персональні дані, якщо пристрій загублено, викрадено або пошкоджено.

Захист мережі WI-FI

Напевно найважливіше у захисті фізичного середовища особистості це захист власне Wi-Fi мережі, у якій функціонують усі девайси.

Далі наведено конкретні поради для підвищення захисту мережі від атак зловмисників.

1) Приховування назви мережі Wi-Fi.

Ім’я мережі або SSID (Service Set Identifier) – це інформація, що відображається при пошуку доступних мереж. Зловмисник, маючи це ім’я, може

виконати підключення до Wi-Fi. Назва мережі повністю відображається при пошуку за замовчування, та регулюється налаштуванням роутера або точки доступу. Для того щоб відключити функцію відображення для роутера, необхідно перейти до розділу «налаштування бездротових мереж» або «Wireless Settings» та обрати опцію «включити SSID» або «відключити SSID».

2) Мережеве шифрування

Опція регулюється також у «налаштуваннях бездротових мереж» та має назву «тип шифрування» або «Encryption settings». Зазвичай користувачу доступні п’ять типів шифрування мережі, але це залежить від типу конкретного роутера.

WEP (WIRED EQUIVALENT PRIVACY) –тип шифрування слабкого рівня. Зловмиснику не знадобиться багато часу для отримання доступу до пристрою Тому таке шифрування взагалі не рекомендують використовувати. WPS / QSS WPS виконує підключення за умови введення коду з 8 цифр. Також протокол WPS має істотні прогалини. Більшість роутерів мають активоване за замовчуванням використання WPS з PIN. Такий PIN-код складається з 4 цифр та підбирається ще швидше, ніж пароль. Тому краще відключити його використання у налаштуваннях роутера.

WPA і WPA2 (WI-FI PROTECTED ACCESS) типи шифрування з підтримкою двох різних режимів аутентифікації при підключенні – PSK і Enterprise. WPA-PSK і Доступ до мережі надається при введені єдиного паролю.

WPA-PSK – має тип шифрування TKIP, WPA2-PSK – AES (шифрування посиленого типу). WPA Enterprise та WPA-PSK є практично однаковими, але для Enterprise необхідне використання RADIUS-серверу, який є службою з віддаленою аутентифікацією, що виконує перевірку облікових даних користувачів для надання доступу.

3) Фільтрація MAC-адрес.

Наступним способом захисту власної мережі є фільтр підключених пристроїв за MAC-адресою, тобто за унікальним мережевим номером. У налаштуваннях роутера слід додати пристрої, які до нього будуть підключені. Якщо MAC-адреса не

відповідає тим, що були вказані при налаштуванні, то пристрою буде відмовлено у доступі до мережі навіть за умови правильно введеного паролю.

Функція має назву «фільтрація MAC-адрес» або «MAC Filtering». Дізнатися цю адресу пристрою можна через термінал операційної системи. Для користувачів Windows потрібно прописати команду ipconfig / all, після чого буде відображена основна мережева інформація пристрою, включно з MAC-адресою. Для операційних систем Unix виконується команда ifconfig.

4) Вимкнення функції віддаленого керування.

Відключати доступ до адміністрування роутера або точки доступу з глобальної мережі Інтернет.

Роутери для Wi-Fi-мереж мають за замовчування активну підтримку функції віддаленого керування з можливістю дистанційного адміністрування через мережу Інтернет. Більшість користувачів таку можливість не використовують. Тому слід її вимкнути, щоб не створювати додаткових можливостей для атак зловмисників.

3.2 Захист особистості в цифровому середовищі

Захист хмарних сервісів

При роботі з хмарою варто дотримуватись певних правил. Нижче наведено поради для підвищення загального рівня захисту.

1) Виконувати перевірку даних та шифрування всіх файлів у закритому доступі.

2) Використовувати лише безпечне з'єднання для підключення до хмарних сервісів.

3) Забезпечити зберігання ключів шифрування в надійному місці, якщо це не виконує постачальник послуг.

4) Використовувати спеціальні програми, призначені для моніторингу даних.

5) Перед збереженням файлів у хмару необхідно їх зашифровувати.

6) Максимально обмежувати завантаження файлів та вкладень з хмарного середовища. Краще зберігати всі документи у хмарі, та не переносити не їх на свій локальний пристрій.

7) Забезпечити захист інтернет-пристроїв.

Для цього слід використовувати технології ідентифікації. Важливо встановлювати паролі достатнього рівня надійності, щоб захистити пристрої від несанкціонованого доступу.

8) Інформування постачальника хмарного сервісу про підозрілі дії.

Відслідковувати фішингові атаки та повідомляти технічну підтримку хмарного сервісу про будь-які підозрілі активності, які було помічено.

9) Адміністрування своїх аккаунтів.

Регулярно перевіряти права доступу до хмарного сховища, а також видаляти облікові записи, які більше не використовуються.

10) Використання технології багатофакторної аутентифікації.

Обов'язкове застосування багатофакторної автентифікації при вході до сервісу хмарних обчислень. Таким чином зловмисники матимуть значно менше шансів для отримання доступу до облікового запису.

Захист при використанні соціальних мереж

Для власного захисту необхідно дотримуватися простих порад, що наведені нижче.

1) Використання надійного паролю для своїх облікових записів.

Переважна більшість атак спричинені використанням паролів недостатньої складності, а також застосуванням єдиного паролю для входу для різних облікових записів. Зазвичай зловмисники використовують метод повного перебору для здійснення атаки. Brute force дозволяє підібрати паролі різного рівня складності протягом декількох хвилин. Також порушники використовують програми, які дозволяють зчитувати натискання на клавіші клавіатури, для збору паролів. Збільшення та ускладнення паролю впливає на кількість можливих комбінацій, а отже і часу на його підбір. Тому використання складного паролю, з комбінацією

маловідомих фраз, чисел та символів, а також слід використовувати унікальну комбінацію для кожного облікового запису.

Менеджер паролів підвищує ефективність парольного захисту. Він допомагає користувачу при створенні нових комбінацій та збереженні вже заданих паролів. З метою покращення безпеки користувачів, компанія Google розробила спеціальні вимоги до паролів для її сервісів, а також надає можливість автозаповнення таким паролем, під час створення, що відповідає усім критеріям надійності.

2) Двофакторна аутентфікація (2FA) — це найбільш простий спосіб для забезпечення безпеки облікових записів у соціальних мережах додатковим рівнем захисту. Такі програми передбачають використання SMS-кодів, повідомлень електронної пошти, та біометричних даних, наприклад відбитків пальців чи сканування обличчя, щоб підтвердити особистість людини.

Переважної більшості атак можливо було уникнути при використанні подібної системи багатофакторної аутентифікації. Оскільки, навіть при зараженні пристроїв через шкідливе програмне забезпечення, зловмисники не мали б можливості отримання доступу до даних.

Соціальні мережі Facebook, Instagram та Twitter надають можливість користування вже вбудованої такої технології та вмикається через налаштування у кожному додатку.

3) Перевірка електронних листів на наявність підозрілої активної при спробах входу.

Зазвичай, соціальні мережі відправляються сповіщення користувачам при спробі несанкціонованого доступу до акаунту. У такому разі для забезпечення захисту, виконується блокування підозрілих спроб входу та сповіщення користувача про необхідність негойної зміни паролю. Тому у випадку такого інформування від соціальних мереж, необхідно діяти швидко для мінімізації можливих наслідків, коли особиста інформація може потрапити до зловмисника.

4) Застережливе використання підозрілих посилань.

Зазвичай, причиною завантаження шкідливого програмного забезпечення, є самі користувачі. Через неуважність до посилань, розміщених у інформаційному

просторі, користувачі стають мішенню зловмисників. Через це, спеціалістами з інформаційної безпеки рекомендовано обережно користуватись посиланнями, що поширені у соціальних мережах, особливо якщо вони мають подібні скорочення як з Bitly або Hootsuite.

Також треба бути обережними до посилань у повідомленнях електронної пошти, які надсилаються нібито від імені соціальної мережі або іншого відомого джерела. Крім цього, у випадках переходу на підозрілу сторінку, яка здається недоречною, рекомендується швидко закрити вкладку браузера і ні в якому разі не натискати ніяких кнопок на цій сторінці. Таким чином можуть здійснюватися атаки виду «клікджекінг», під час яких зловмисники використовують приховані елементи на веб-сторінках для маніпуляції діями користувача і в подальшому отримання доступу до його даних.

5) Обмеження при поширенні особистих даних в соцмережах.

Для безпеки акаунту важливим є контроль публікування персональної інформації про себе та своїх друзів. Крім цього, слід пам’ятати про можливості налаштування конфіденційності особистого профілю. Сторінка користувача може бути відкритою для всіх віртуальних друзів, незалежно від їх взаємозв’язку.. А отже, загальнодоступна інформація може використовуватись зловмисниками з шахрайською метою, зокрема методами соціальної інженерії .

Захист при використанні електронної пошти

Електронна пошта широко використовується по всьому світу для пересилання особистих листів чи робочої документації. Але, далеко не кожен користувач пошти задумується про те, що конфіденційність його інформації може опинитися під загрозою. Це дійсно так, оскільки отримання доступу до чиєїсь скриньки ставить під загрозу усі облікові записи, зареєстровані за цією поштою.

Варто зауважити, що не існує 100% надійного способу захисту персональних даних електронної пошти. Проте можна використовувати наведені нижче поради, які значно підвищать рівень захисту.

1) Правильний вибір сервісу.

Використання відомих поштових сервіси, наприклад Gmail, Outlook, чи Yahoo Mail, забезпечує користувачів набором інструментів для захисту. Такі інструменти надають можливість використання технології двофакторної аутентифікації з ключами безпеки. Не рекомендовано вказувати адресу основної поштової скриньки при реєстрації на різних сайтах. Оскільки це сприяє збільшенню ризику порушення конфіденційності інформації. Натомість, варто створити кілька акаунтів на сервісах електронної пошти. Один обліковий запис для особистого листування з друзями і близькими, другий – для листування по робот, третій – для реєстрації на сайтах і сервісах, четвертий – для клієнтів і публікації рекламної продукції. Звісно, це призведе до виникнення певних незручностей у користуванні, але значно зменшить ризики. Слід також використовувати наскрізне шифрування, особливо при відправці конфіденційних даних.

2) Наступний спосіб захисту персональних даних – створення одноразових адрес.

Одноразові поштові адреси - це комбінації випадкових букв і цифр. Їх можна застосовувати для реєстрації на сайтах, з можливістю налаштувавши переадресації листів на основну пошту. Найкращий генератор анонімної електронної пошти – Burner Mail. Завдяки цьому сервісу, рекламодавці не можуть відстежувати дії клієнта в мережі. Аналогічні опції мають сервіси Apple і Firefox. Для використання такої функції слід увімкнути опцію “приховати електронну пошту”, щоб створювалися одноразові “поштові скриньки”. В більшості випадків такі облікові записи видаляться через 10 хвилин.

2) Встановлення брандмауера та ефективних антивірусних програм.

3) Контроль доступу до комп’ютера або смартфону та використання.

4) Використання методів шифрування при відправці важливих даних.

Це забезпечить захист інформації і навіть, при перехопленні листів зловмисником, не дозволить отримати доступ до вмісту.

5) Використання фільтрів для спаму.

Існують спеціальні можливості фільтрації листів електронної пошти. Завдяки таків фільтрації, усі підозрілі листи відправляються одразу до категорії «спам», та через певний проміжок часу автоматично видаляються.

Захист браузера

Далі перераховані рекомендації для захисту інформаційної безпеки особистості від можливих загроз через браузер.

1) Регулярне оновлення браузеру.

Для підвищення рівня захисту браузер має бути правильно оновлений. Оскільки розробники з кожним наступним оновленням підвищують виправляють недоліки та підвищують рівень захисту. Зазвичай це відбувається автоматично, але можуть з’являтися помилки, і інколи необхідно оновлювати браузер вручну.

У разі Google Chrome перейдіть до меню у верхньому правому куті, натисніть «Довідка» та «Інформація про Google Chrome». Він автоматично покаже, яку версію ви встановили, і, якщо є новіша, автоматично розпочне встановлення. Щось подібне відбувається з іншими браузерами, такими як Firefox. Вам також потрібно перейти до Довідки, ввести «Про Firefox» та натиснути оновлення.

2) Використання захисного програмного забезпечення.

Звичайно, щоб підтримувати безпеку та запобігати атакам на браузер, завжди повинні бути встановлені програми безпеки. Важливо мати хороший антивірус, Наприклад, Windows Defender або будь-яка інша альтернативна програма.

Але крім використання антивірусу, також можна розраховувати на інші програми безпеки, такі як брендмауер або навіть розширення для браузера. Існують спеціальні плагіни для підтримки безпеки та запобігання атак, наприклад WOT або HTTPS Everywhere, які допомагають підтримувати конфіденційність.

3) Безпечне встановлення плагінів.

Якщо ви збираєтеся встановити будь-яке розширення, навіть безпечне, як ми показали, важливо, щоб ви встановили їх безпечно. Ви завжди повинні відвідувати офіційний магазин браузерів, будь то Chrome, Firefox або той, який ви використовуєте. Вам слід уникати встановлення плагінів із незахищених джерел.

Зловмисник може створити підроблене розширення або змінити законне розширення, щоб вкрасти дані.

4) Обережне відвідування веб-сторінок.

Це, напевно, найважливіша рекомендація. Насправді, можна сказати, що більшість атак вимагає помилки від самого користувача. Наприклад, натиснути шкідливе посилання, завантажити файл, який насправді є шкідливим програмним забезпеченням, встановити підроблений плагін для браузера тощо.

Для того, щоб цього уникнути, необхідно входити на надійні сайти та бути обережними під час завантаження файлів або встановлення чогось. Це запобіжить багато типів атак на браузер, які можуть поставити під загрозу дані та їх належне функціонування.

5) Уникати використання небезпечних мереж.

Деякі атаки, як-от Man in the Browser, можуть з’явитися, коли ми підключаємося до небезпечних мереж Wi-Fi. Тому важливо уникати тих, які можуть бути небезпечними. Наприклад, мова йде про мережі Wi-Fi в громадських місцях, таких як аеропорт чи торговий центр.

Якщо необхідно підключитися до ненадійного сайту, можна скористатися сервісом VPN. Такі програми виконують шифрування з’єднання та дозволяють захищати особисті дані під час перегляду в мережі. Сервіси виконують підключення до небезпечної мережі через свою приватну мережу. Гарними варіантами таких застосунків для простих користувачів є наприклад NordVPN та ExpressVPN.

Захист при використанні Web-застосунків

Веб-застосунок (англ. Web Application) — це застосунок, у якому клієнтом виступає браузер, а сервером — веб-сервер.

Рекомендації для захисту Web-додатків для користувача також є досить простими.

1) Використання HTTPS.

Використання протоколу HTTPS гарантує цілісність і конфіденційність взаємодії з сервером, захищає дані при передачі в мережі Інтернеті. Сертифікат має бути виданий центром сертифікації.

Переглядаючи веб-сторінки з будь-якого пристрою, переконайтеся в тому, що ваше з’єднання захищене за протоколом HTTPS. Ви завжди можете перевірити, чи це так, подивившись на початок інтернет-адреси.

2) Правильне налашування браузера.

Злом сайту починається зі збору інформації про сервер, тому правильне налаштування браузера є надзвичайно важливим. Важливо при цьому зауважити, що ніколи не можна зберігати у браузері або застосунках імена користувачів та паролі.

3) Ретельна перевірка адрес сайтів, перед їх використанням.

Перш ніж увійти в систему або надіслати конфіденційну інформацію, переконайтеся у правильності веб-адреси, оскільки зараз існує величезна кількість підробних сайтів та веб-застосунків.

Висновки до розділу 3

На основі побудованої моделі порушника було розроблено методичні рекомендації для інформаційно-технічної складової для забезпечення інформаційної безпеки. Ці рекомендації призначені для різних категорій населення і мають на меті допомогти людині забезпечити власну безпеку у інформаційному середовищі.

ВИСНОВОК

Аналіз різних аспектів безпеки особистості в інформаційному середовищі, дав мені необхідну інформацію для розробки технічних рекомендацій для забезпечення потреб інформаційної безпеки особистості.

Спочатку був проведений аналіз теоретичних аспектів інформаційної безпеки в цілому та інформаційної безпеки безпосередньо особистості. Також був проведений аналіз нормативно-правової бази у інформаційній сфері. На даний момент, питання інформаційної безпеки особистості не має чіткого визначення та розглядається лише дотично до інших проблем інформаційної безпеки. Було проведено аналіз та було визначено основні закони, які в тій чи іншій мірі розкривають поняття інформаційної безпеки особистості у правовому полі. Виконання цього завдання дало гарну основу для подальшого дослідження.

Під час наступного завдання було проведено дослідження можливих загроз для особистості, а також аналіз основних видів атак. Інформація, отримана у ході дослідження, була використана для побудови моделі порушника інформаційної безпеки особистості. У дипломній роботі представлено детальний описом цієї моделі.

На основі створеної моделі порушника було розроблено технічні рекомендації та конкретні поради для забезпечення інформаційної безпеки особистості самою особистість. На жаль, ніякі засоби на даний момент, не здатні забезпечити абсолютного захисту від інформаційних загроз. Проте, використання розроблених під час дипломного проектування, рекомендацій може значною мірою підвищити рівень захисту безпеки особистості в цілому у інформаційному середовищі.

Стрімкий розвиток інформаційних технологій здійсню вплив майже на кожну сферу нашої життєдіяльності. Використання таких технологій надає людині нові величезні можливості. Але зі збільшення можливостей збільшується рівень і загроз. Забезпечення інформаційної безпеки особистості в першу чергу залежить від самої особистості, а вже потім від інших чинників. Зараз більшість людей досі

залишаються малозахищеними або зовсім не захищеними в інформаційному суспільстві.

Розроблені мною рекомендації щодо захисту інформаційної безпеки особистості призначені для самої особистості. Використання цих рекомендацій має на меті допомогти людині забезпечити захист власної інформаційної безпеки від основних видів загроз, які можуть виникнути у інформаційному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Загрози для мобільних пристроїв [Електронний ресурс]. – Режим доступу: https://studref.com/325282/informatika/ugrozy_mobilnyh_ustroystv.

2. Сучасні загрози мобільним пристроям та їх захист [Електронний ресурс]. – Режим доступу: https://www.anti-malware.ru/analytics/Threats_Analysis/keeping-mobile-devices-safe-from-cyber-threats.

3. Види атак та загроз у браузері, як захиститись [Електронний ресурс]. – Режим доступу: https://itigic.com/ru/types-of-attacks-and-threats-in-the-browser-and-how-to-be-protected/.

4. На руці, але не в безпеці: як хакери атакують смарт-годинники [Електронний ресурс]. – Режим доступу: https://eset.ua/ua/blog/view/131/na-ruke-no-ne-v-bezopasnosti-kak-khakery-atakuyut-smart-chasy.

5. ЗАГРОЗИ І ВРАЗЛИВОСТІ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ [Електронний ресурс]. – Режим доступу: https://naukam.triada.in.ua/index.php/konferentsiji/70-tridtsyat-dev-yata-vseukrajinska-praktichno-piznavalna-internet-konferentsiya/933-zagrozi-i-vrazlivosti-bezpeki-rozumnogo-budinku.

6. Як покращити захист акаунта в соціальних мережах– практичні поради [Електронний ресурс]. – Режим доступу: https://eset.ua/ua/blog/view/50/kak-uluchshit-zashchitu-akkaunta-v-sotsialnykh-setyakh-prakticheskiye-sovety

7. Як захистити пошту від злому? [Електронний ресурс]. – Режим доступу: https://datami.ua/yak-zahistiti-poshtu-vid-zlamu/.

8. Тема 9. Інформаційна безпека [Електронний ресурс]. – Режим доступу: http://jure.in.ua/tema-9-informatsijna-bezpeka/.

9. АНАЛІЗ КОНЦЕПЦІЙ ВИЗНАЧЕННЯ «ІНФОРМАЦІЙНОЇ БЕЗПЕКИ» В УМОВАХ ГЛОБАЛІЗАЦІЇ [Електронний ресурс]. – Режим доступу: https://social-science.uu.edu.ua/article/1400.

10. ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА ОСОБИСТОСТІ [Електронний ресурс]. – Режим доступу: https://www.pdau.edu.ua/ sites/ default/ files/node/2795/15stattyarublykyuo.pdf.

11. FUNCTIONS OF THE INDIVIDUAL INFORMATION SECURITY IN SOCIETY [Електронний ресурс]. – Режим доступу: http://pag-journal.iei.od.ua/ archives/2019/13-2019/25.pdf.

12. ІНФОРМАЦІЙНІ ПРАВА І СВОБОДИ ЛЮДИНИ І ГРОМАДЯНИНА В УКРАЇНІ: ВИЗНАЧЕННЯ ТЕРМІНІВ, СПІВВІДНОШЕННЯ ПОНЯТЬ [Електронний ресурс]. – Режим доступу: http://ippi.org.ua/sites/default/files/4_8.pdf

13. Хворост Х.Ю. Інформаційно-психологічний вплив в розрізі безпеки здоров'я. Наука і освіта. 2016. № 2-3. С. 184–191.

14. ЛЮДСЬКА ПСИХІКА В ІНФОРМАЦІЙНІЙ НЕБЕЗПЕЦІ [Електронний ресурс]. – Режим доступу: https://doi.org/10.32838/TNU-2663-6468/2020.3/39.

15. ЗОЛОТАР О.О. Інформаційна безпека людини:теорія і практика : монографія. – Київ : ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

16. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю.Кондратьєва. – К., 2004.

17. Актуальні кіберзагрози 2021 рік [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/.

18. Вразливості хмарної інфрастуктури [Електронний ресурс]. – Режим доступу: https://habr.com/ru/company/cloud4y/blog/500866/.

19. Захист електронної пошти [Електронний ресурс]. – Режим доступу: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/zaschita-elektronnoj-pochty/.

20. Потенційні загрози інформації, що оброблюється персональними комп'ютерами [Електронний ресурс]. – Режим доступу: https://studref.com/ 482407/ informatika/potentsialnye_ugrozy_informatsii_obrabatyvaemoy_personalnyh_kompyuterah.

21. Потенційні загрози інформації, що оброблюється персональними

комп’ютерами [Електронний ресурс]. – Режим доступу: https://studopedia.su/13_114921_potentsialnie-ugrozi-informatsii-obrabativaemoy-v-personalnih-kompyuterah.html.

22. Чек-лист реагування на інциденти, пов'язані з електронною поштою [Електронний ресурс]. – Режим доступу: https://softprom.com/ua/chek-list-reaguvannya-na-intsidenti-povyazani-z-elektronnoyu-poshtoyu.

23. Основні цілі та об'єкти інформаційної безпеки особистості. Джерела загроз інформаційній безпеці. Основні завдання забезпечення інформаційної безпеки особистості. [Електронний ресурс]. – Режим доступу: https://consultingbnp.ru/ uk/microsoft-office/osnovnye-celi-i-obekty-informacionnoi-bezopasnosti-lichnosti/.

24. WFP Guide to Personal Data Protection and Privacy [Електронний ресурс]. – Режим доступу: https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/.

25. Забезпечення інформаційної безпеки в країнах Центральної Європи . УДК 342 4: 327. 7

26. Закон України «Про інформацію» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

27. Закон України «Про доступ до публічної інформації» [Електронний ресурс].Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

28. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

29. Закон України «Про захист суспільної моралі» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1296-15#Text.

30. Закон України «Про захист персональних даних» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.