Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
випускної кваліфікаційної 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: Методи та умови реалізації політики конфіденційності та захисту персональних даних в соціальних мережах

Виконавець: студентка IV курсу, групи КБ-42
Катерина РУДЕНКО
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Микола БРАЙЛОВСЬКИЙ	

Нормоконтроль	Сергій ДАКОВ	

Київ 2022

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач 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** **Руденко Катерини Сергіївни**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Методи та умови реалізації політики конфіденційності та захисту персональних даних в соціальних мережах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

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

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Модульні алгоритми захисту, методи аутентифікації, механізми захисту від несанкціонованого доступу, алгоритми шифрування.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитись з нормативно-правовою базою, проаналізувати основні джерела загроз, дослідити оцінку ризиків, розглянути методи захисту персональних даних, розробити рекомендації від несанкціонованого доступу.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність .Розроблені рекомендації дипломної роботи можуть бути використані задля підвищення рівня безпеки в соціальних мережах.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2022 року.

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Катерина. РУДЕНКО
(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	23.01.2022 – 12.02.2022	*виконано*
3	Огляд правової документації	12.02.2022 - 23.02.2022	*виконано*
4	Аналіз основних джерел загроз	16.03.2022 - 26.03.2022	*виконано*
5	Дослідження оцінки загроз в соціальних мережах	26.03.2022 – 07.04.2022	*виконано*
6	Аналіз існуючих методів захисту персональних даних	08.04.2022 – 19.04.2022	*виконано*
7	Побудова модульного алгоритму від несанціонованого доступу	20.04.2022 – 01.05.2022	*виконано*
8	Формування рекомендацій з підвищення захищенності персональних даних	01.05.2022 – 26.05.2022	*виконано*
9	Оформлення пояснювальної записки	05.06.2020 – 08.06.2020	*виконано*
10	Підготовка до захисту дипломної роботи	08.06.2022 – 13.06.2022	*виконано*

Студент-дипломник _____ Катерина. РУДЕНКО
(підпис) (ініціали, прізвище)

Керівник випускної кваліфікаційної роботи _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 09.06.22.

УДК 004.056.5:004.94

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Методи та умови реалізації політики конфіденційності та захисту персональних даних в соціальних мережах» складається зі вступу, основної частини, що містить 3 розділи, висновків і списку літератури та джерел. Загальний обсяг роботи – 61 сторінки. Робота містить 9 таблиць, 9 рисунків. Список використаних джерел включає 32 джерела.

Метою дослідження є створення політики конфіденційності та захисту персональних даних в соціальних мережах.

Об'єктом дослідження є процес підвищення захищеності даних в соціальних мережах шляхом вдосконалення існуючої політики безпеки.

Предметом дослідження є політика конфіденційності та захисту персональних даних в соціальних мережах.

Методи дослідження. При написанні дипломної роботи були застосовані метод аналізу, метод порівняння, метод синтезу.

Практичне значення отриманих результатів полягає у можливості впровадження розробленої політики безпеки в соціальні мережі з метою захисту персональних даних.

Ключові слова: персональні дані, джерела загроз, загроза, оцінка ризиків, ресурс, рівень загроз, несанкціонований доступ, рекомендації, метод захисту.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ЗУ	–	Закон України
ЕЦП	–	Електроний цифровий підпис
ПЗ	–	Програмне забезпечення
АС	–	Автоматизовані системи
СКУД	–	Система контроля і управління доступом
ОС	–	Операційні системи
DLP	–	Data Leak Prevention
SOC	–	Security Operations Center
SIM	–	Security Information Management
SEM	–	Security Event Management
SIEM	–	Security Information and Event Management
CSS	–	Cascading Style Sheets
HTML	–	Hypertext Markup Language
ПД	–	Персональні дані

ЗМІСТ

ВСТУП

Застосування досягнень науково-технічного прогресу та сучасних інформаційних технологій надає суспільству неабиякі можливості задля спілкування. Завдяки передовим Інтернет-технологіям існує змога в пару кліків та за декілька секунд зв'язатися із будь-ким, хто знаходиться хоч на боці Землі. Сучасні мережі об'єднують людей для обговорення різноманітних питань, дозволяють встановлювати та широко використовувати соціальні контакти. Одними із таких засобів спілкування є соціальні мережі.

З метою вдосконалення законодавчого захисту прав людей на приватне життя на рівні міжнародного права, важливим є розгляд витребуваних та суперечних питань щодо обробки й захисту персональних даних у соцмережах, а також віднаходження оптимальних шляхів щодо їх врегулювання.

Дослідженням певних питань даної проблематики в українській юридичній літературі у різні періоди займалися М. Різак, В. Брижко, В. Панченко, О. Радкевич, А. Марущак тощо. Це питання розглянути також і такі зарубіжні вчені як А. Міллер, І. Вельдер, Р. Холлборг.

Порушену проблематику вивчало чимало науковців, проте велика кількість її аспектів й донині лишаються недостатньо дослідженими або дискусійними, зокрема в контексті становлення в даній сфері українського законодавства.

Метою написання дипломної роботи є створення політики конфіденційності та захисту персональних даних в соціальних мережах.

При написанні роботи були поставлені наступні *завдання*:

1. Виконати огляд предметної області та показати актуальність захисту персональних даних в соціальних мережах.

2. Дослідити існуючі механізми та методи захисту персональних даних в соціальних мережах.

3. Розробити рекомендації з підвищення захищеності даних в соціальних мережах.

Об’єкт дослідження – процес підвищення захищеності даних в соціальних мережах шляхом вдосконалення існуючої політики безпеки.

Предмет дослідження – політика конфіденційності та захисту персональних даних в соціальних мережах.

Були застосовані наступні **методи дослідження**:

- метод аналізу;
- метод порівняння;
- метод синтезу.

Отримані результати мають практичне значення, що полягає в можливості впровадження розробленої політики безпеки в соціальні мережі з метою захисту персональних даних.

РОЗДІЛ 1
ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ. АКТУАЛЬНІСТЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

1.1 Аналіз законодавства України, що регулює захист інформації

Правова форма захисту інформації полягає у застосуванні законів та статей Конституції держави, положень кримінального, цивільного кодексів, а також інших нормативно-правових документів в сфері захисту інформації, інформаційних відносин та інформатики загалом. Дана форма захисту закріплює права та обов’язки сторін, що перебувають у інформаційних відносинах, регламентує правовий статус органів, технічних методів та засобів захисту інформації, а також являє собою базу задля встановлення морально-етичних норм в даній сфері [1].

Захист інформації з правової точки зору є загальновизнаним на міжнародному й державному рівнях. У першому випадку існує чимало міжнародних договорів, угод, конвенцій та декларацій, а у другому — правовий захист підлягає регуляції державними, а також відомчими нормативно-правовими актами.

Система законодавчих актів і нормативних, адміністративних, організаційних документів, що була розроблена на їх базі, має забезпечувати організацію результативного контролю їх виконання правоохоронними органами та використання на практиці засобів захисту і відповідальності сторін інформаційних відносин. Дану систему можна відносити до морально-етичних норм поведінки суб’єктів, що історично склалися чи розвиваються разом із розповсюдженням обчислювальних засобів у сучасному соціумі.

В Україні існують наступні законодавчі документи, що регламентують захист інформації:

- Стаття 31 Конституції України;

- Закон України (ЗУ) «Про інформацію»;
- ЗУ «Про Національну програму інформатизації»;
- ЗУ «Про захист персональних даних»;
- ЗУ «Про електронний цифровий підпис»;
- ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах»;
- ЗУ «Про електронні документи та електронний документообіг»;
- ЗУ «Про державну таємницю»;
- Положення про порядок здійснення криптографічного захисту інформації в Україні.

Державна політика в області захисту інформації реалізується Державною службою спеціального зв'язку та захисту (Держспецзв'язок) інформації України відповідно до закону.

Зупинимося для більш детального розгляду на наведених вище законодавчих документах.

В ЗУ "Про інформацію" [2] встановлено право громадян держави на інформацію, а також закладено низку правових основ інформаційної діяльності України.

Даний ЗУ визначає статус учасників інформаційних відносин, захищає від неправдивості даних та розповсюджується на будь-які інформаційні відносини всіх сфер життя та діяльності суспільства й держави. До законодавства України про інформацію входять не лише зазначений закон, але й Конституція України, законодавчі акти певних галузей, видів, засобів та форм інформації, а також міжнародні угоди, договори, що були ратифіковані Україною, і принципи та норми міжнародного права.

Поняттю «інформація» за цим Законом відповідають будь-які дані чи відомості, що може зберігатися у задокументованому на носіях чи опублікованому вигляді, в тому числі в електронній формі.

Закон України «Про державну таємницю» визначає соціальні відносини, що взаємопов'язані з ототожненням інформації до категорії державної таємниці, а

також засекречуванням та розсекречуванням матеріальних носіїв даної інформації та захистом державної таємниці, тримаючи на меті захист національної безпеки держави.

Згідно до Закону України «Про електронний цифровий підпис» він «…визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

Електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів. ЕЦП використовується фізичними та юридичними особами - суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі…»[5].

Закон України «Про національну програму інформатизації» [6].

Даний Закон розглядає основні положення щодо формування, впровадження та внесення корективів у Національну програму інформатизацію, що визначає шлях вирішення проблеми забезпечення інформаційних потреб та забезпечення інформацією оборонної, науково-технічної, соціально-економічної, екологічної, національно-культурної діяльності й інших її видів в масштабах державного значення.

Закон України «Про захист персональних даних» — є суспільно-політично важливим та значущим для України та лише підтверджує позитивні демократичні зрушення в суспільстві, інтеграції в нашій державі кращих правових здобутків сучасного людства.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Він має на мені гарантування метою забезпечення суворого дотримання прав власності як фізичних, так і юридичних осіб на захист інформації, а також доступу до неї. Власне захист інформації у системі реалізується завдяки застосуванню багатокомпонентної системи захисту інформації. Також для цього використовується дотримання суб'єктами відносин законодавства України й усіх нормативно-правових документів у даній сфері. Використовуються електронно-обчислювальна техніка, ПЗ (програмне

забезпечення), телекомунікаційне обладнання, інструменти захисту інформації в системі, відповідні до вимог законів України стосовно захисту інформації [8].

Положення про порядок здійснення криптографічного захисту інформації в Україні. «Це Положення визначає порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої завдає (може завдати) шкоди державі, суспільству або особі» [9].

Стаття 31 Конституції України затверджує: «Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановленні лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо» [10].

В цій статті також проголошується, що жодна людина захищається законом від безпідставного посягання на конфіденційність її кореспонденції, та зазначаються конкретні форми листування (до «іншої кореспонденції» слід відносити електронну пошту. Таємницю листування відносять до особистих таємниць кожної окремої людини.

1.2 Актуальність забезпечення інформаційної безпеки. Оцінка ризиків

З ростом можливостей інформаційних технологій усвідомлюється важливість захисту персональних даних.

Беручи до уваги тенденцію до вдосконалення захисту приватного життя на рівні міжнародного права, вкрай важливим нині вбачається розгляд й вивчення актуальних та суперечних питань оброблення та захисту персональних даних у соцмережах, а також пошук більш оптимальних способів їх врегулювання у полі вітчизняного права [14].

Архітектура інформаційної безпеки повинна пропонувати структуру, на якій аналізуються вимоги безпеки, ризики і загрози, а також складається портфель кращих інтегрованих рішень безпеки.

Основна мета системи інформаційної безпеки - створити систему, яка спрямована на задоволення потреб в безпеці в трьох ключових областях як критичних систем, так і даних: цілісність, конфіденційність і доступність.

Актуальність забезпечення інформаційної безпеки для соціальних мереж доведемо на аналізі ризиків.

Здійснюючи аналіз та класифікацію джерел саме загроз інформації, припускаємо, що навіть одна й та сама загроза може потребувати різні методи відображення для зовнішніх і внутрішніх джерел.

Окрема група внутрішніх джерел — спеціально впроваджені, завербовані агенти, що були залучені з основного, допоміжного та технічного персоналу, а також з працівників відділу інформаційної безпеки.

Всі джерела загроз було диференційовано на такі групи:

–антропогенні — помилки, що сталися під час експлуатації, проектування чи розробки компонентів АС, а також навмисні дії злочинців;

–техногенні — різноманітні аварії, порушення в ході роботи, відмови технічних засобів;

–обумовлені стихійними лихами чи катаклізмами.

Зазначена класифікація та перелік джерел ймовірних загроз, що властиві об'єкту інформатизації, наведені у таблицях 1.1 та 1.2.

Таблиця 1.1

Антропогенні джерела загроз системи

№	Зовнішні антропогенні джерела	№	Внутрішні антропогенні джерела
1.	Кримінальні групи	1.	Працівники
2.	Потенційні злочинці	2.	Адміністратори АС
3.	Персонал постачальників	3.	Технічний персонал
4.	Представники наглядових організацій і аварійних служб	4.	Працівники відділу безпеки

До антропогенних джерел загроз відносяться суб'єкти, що володіють санкціонованим або несанкціонованим доступ до роботи інформаційних

систем, чиї дії яких можуть призвести до умисних чи вчинених із необережності проблем.

Група антропогенних джерел загроз цікавить найбільше, адже дії суб'єкту є змога оцінити, передбачити та вжити щодо них необхідні заходи (таблиця 1.2).

Таблиця 1.2

Техногенні джерела загроз

№ п / п	Зовнішні техногенні джерела загроз	№ п / п	Внутрішні техногенні джерела загроз
1.	Засоби зв'язку, промислові установки іонізуючого випромінювання, системи енергозабезпечення	1.	Неякісні технічні засоби обробки інформації
2.	Мережі інженерних комунікацій (Водопостачання, каналізації)	2.	Неякісні програмні засоби обробки інформації
3.	Транспорт (авіаційний, залізничний, автомобільний, водний)	3.	Допоміжні засоби (Охорони, сигналізації, телефонії, відеоспостереження, СКУД)
4.		4.	Інші технічні засоби

Техногенні джерела загроз зумовлюються технократичною діяльністю людей та розвитком техніки.

Стихійні джерела загроз об'єднуються обставинами, що мають об'єктивний та абсолютний характер. Їх неможливо передбачити чи запобігти одночасно, через це захисні заходи від загроз даного порядку мають застосовуватися постійно, адже спрогнозувати їх неможливо.

Наразі обробка даних, враховуючи комерційну таємницю, проводиться в режимі, що розрахований на велику кількість користувачів із розподіленими правами доступу.

Аналізуючи ризик, вивченню підлягають складові інформаційної системи, що здатні піддатися певним загрозам — вони вказують на вразливі місця системи, допомагають оцінити вірогідність реалізації кожної окремої

загрози та зорієнтувати щодо розмірів втрат. Також вони вибирають потенційні методи захисту та роблять розрахунки їх вартості.

Заключний етап аналізу — оцінка потенційної вигоди, яку можна буде отримати завдяки застосуванню заходів захисту, що можна передбачити. Зазначена вигода може бути позитивною чи негативною за значенням.

Розрахунок коштовності збитку є одним з найбільш вагомих факторів аналізу ймовірних ризиків й економічного обґрунтування фінансових витрат на забезпечення інформаційної безпеки (в соцмережах у тому числі). Адже витрати мають не перевищувати вартість об'єкта, що захищає, чи обсяг збитків.

Враховуючи, що співробітники підприємств можуть на робочих місцях здійснювати вхід до соціальних мереж, варто розглянути аналіз ризиків і з цієї точки зору.

Пропонується застосовувати спрощену модель розрахунку розміру збитків.

Вартість втрат, що можуть бути отримані через зниження продуктивності працівників атакованого вузла чи сегмента розраховується наступним чином [14]:

$$П_{П} = \frac{\sum_{N_C} Z_C}{192} \times t_{П}, \qquad (1.1)$$

де $П_П$ – втрата продуктивності;

$t_П$ – це час простою (періоду, коли робота неможлива) через атаку;

Z_C – зарплатня робітників атакованого сектору;

N_C – кількість робітників атакованого сектору.

Затрати на відновлення нормальної працездатності вузла або сегмента, що був атакований, складається з декількох елементів:

$$П_В = П_{ВІ} + П_{ВВ} + П_{Зч}, \qquad (1.2)$$

де $П_В$ – вартість відновлення працездатності вузла чи сегмента, що був атакований;

$П_{ВІ}$ – вартість введення інформації наново;

$П_{ПВ}$ – вартість його відновлення, перевстановлення системи, конфігурація тощо;

$П_{Зч}$ – вартість заміни технічного забезпечення, обладнання, запасних частин.

$$П_{ВІ} = \frac{\sum Z_C}{\frac{N_C}{192}} \times t_{ВІ}, \quad (1.3)$$

де $t_{ВІ}$ – час повторного введення втраченої інформації;

Z_C – зарплата співробітників атакованого вузла чи сегмента;

N_C – кількість робітників атакованого вузла чи сегмента.

$$П_{ПВ} = \frac{\sum Z_O}{\frac{N_0}{192}} \times t_В, \quad (1.4)$$

де $t_В$ – час відновлення роботи після атаки;

$Z_о$ – зарплатня обслуговуючого персоналу;

$N_О$ – число обслуговуючого персоналу.

Упущена вигода через простій атакованого вузла чи сегмента дорівнює:

$$U = П_П + П_В + V, \quad (1.5)$$

де U – втрачена вигода через простій вузла / сегмента;

$$V = \frac{О}{52 \times 5 \times 8} \times (t_П + t_В + t_{ВІ}), \quad (1.6)$$

де tП – час простою через атаку;

$t_В$ – час відновлення роботи після атаки;

$t_{ВІ}$ – час введення втраченої через атаку інформації наново;

Отже, загальний збиток через атаки на елемент мережі (в т. ч. й по причині несанкціонованого доступу до соціальної мережі) складе:

$$OY = \sum_{год} \sum_{t} U, \tag{1.7}$$

Інтерпретація моделі розрахунку адекватно виконується відповідним чином:

а) об'єктом захисту,

б) ймовірним інцидентом.

Ризиком називається сукупність можливих подій та їх наслідків; ймовірністю – міра того, що певна подія може статися; оцінкою ризику – загальний аналіз ризику й оцінка ризику.

Математичне визначення ймовірності: дійсне число в інтервалі від 0 до 1, що відносяться до випадкової події.

Коли ступінь впевненості достатньо висока, ймовірність наближується до одиниці. Частіше за все зустрічається два способи тлумачення ймовірності: об'єктивна та суб'єктивна.

Об'єктивна (фізична) ймовірністю — це відносна частота реалізації якого-небудь явища в загальному обсязі спостережень чи відношення числа сприятливих результатів до загальної кількості спостережень.

Дане поняття використовується у аналізі результатів чисельних спостережень, які відбувалися в минулому чи отриманих в якості результатів з моделей, що описують певні процеси.

Суб'єктивна ймовірність — міра впевненості людини чи групи людей у тому, що дане явище здійсниться.

Частіше за все часто вона являє собою вірогідну міру, що отримується емпіричним шляхом, на розділяється на три етапи:

- підготовчий етап,

- етап отримання оцінок,

- етап аналізу оцінок.

На першому, підготовчому, етапі формується об'єкт дослідження – певна множина подій, та проводиться підготовка експерта чи групи експертів та ознайомлення їх із методом.

Другий етап — застосування методу, що було обрано на підготовчому етапі. Результатом буде набір конкретних чисел, що відображає суб'єктивне бачення експерта чи групи експертів на вірогідність тієї чи іншої події, хоча не завжди може вважатися остаточним розподілом, адже нерідко містить суперечності.

Третій етап — дослідження результатів опитування. Якщо представлені експертами ймовірності не відповідають аксіомам ймовірності, то відповіді експертів мають ще уточнюватися та приводитися у відповідність вибраній системі аксіом.

Індивідуальність аналізу інформаційних ризиків для кожного конкретного випадку злому соціальної мережі обумовлена також тим, що обсяг збитків пов'язаний з кількістю інформаційних ресурсів та унікальною для кожного підприємства оцінкою їх важливості.

Для цієї роботи найбільший інтерес мала ситуація, коли співробітник використовує соціальну мережу, працюючи в організації.

Гарантувати безпеку інформації всередині організації можливо тільки в разі наявності та суворому дотриманні правил захисту інформації, які чітко регламентують, яку саме інформацію, де та яким шляхом необхідно захищати, а також діючих для усіх співробітників без винятку.

Критичність визначається тим, наскільки небезпечним для бізнесу є порушення конфіденційності, цілісності чи доступності.

Рівень критичності ресурсу можна визначити у вигляді таблиці 1.3.

Таблиця 1.3

Рівень критичності ресурсу

Назва рівня	Визначення в грошових одиницях	Визначення з точки зору впливу на репутацію компанії
Низький рівень	Незначний збиток	Незначний вплив
Середній рівень	Помітний (великої шкоди)	Істотний вплив
Високий рівень	Значної шкоди	Шкода, що може завадити продовженню подальшої діяльності

Під простотою реалізації загрози розуміється наступне (таблиця 1.4).

Таблиця 1.4

Реалізація загрози

Реалізація загрози	Необхідні для реалізації знання
Низька	Немає детальних знань про принципи функціонування системи; може бути реалізована будь-яким користувачем
Середня	Висока кваліфікація, навички в програмуванні, наявність прав адміністратора, знання про помилки в реалізації ПЗ
Висока	Знання помилок в реалізації ПЗ, знання вихідного коду, високі навички програмування, значні матеріальні та часові ресурси, привілеї адміністратора

Під критичністю реалізації загрози мається на увазі ступінь її впливу на ресурс (таблиця 1.5).

Таблиця 1.5

Критичність реалізації загрози

Критичність реалізації загрози	Опис
Висока	Інформація втрачена чи спотворена, доступ до ресурсу повністю заблоковано
Середня	Зловмисники отримали інформацію для здійснення атак в майбутньому, доступ до ресурсу важко чи лише тимчасово заблоковано
Низька	Зловмисники отримали суттєву (з точки зору реалізації подальших атак) інформацію про ресурс

Оцінка ризику.

Спочатку необхідно розрахувати рівень загрози по уразливості Th на базі критичності а вірогідності реалізації загрози через конкретну уразливість.

Рівень загрози демонструє, чи є критичним вплив цієї загрози на ресурс з урахуванням ймовірності її реалізації та наскільки:

$$\mathrm{Th} = \frac{\mathrm{ER}}{100} \times \frac{\mathrm{P}(V)}{100}, \tag{1.8}$$

де ER - критичність реалізації загрози (задається в відсотках);

P (V) - вірогідність реалізації загрози через певну уразливість (задається в відсотках).

Отримуємо значення рівня загрози по уразливості в інтервалі від 0 до 1.

Для розрахунку рівня загрози за всіма загрозами CTh необхідно підсумувати отримані рівні загроз через конкретні уразливості за допомогою наступної формули:

$$\mathrm{CTh} = 1 - \prod_{i=1}^{n} (1 - \mathrm{Th}_i), \tag{1.9}$$

де Th - рівень загрози по уразливості.

Значення рівня загрози по всім уразливостям становитиме 0 - 1.

Розрахуємо загальний рівень загроз по ресурсу CThR (із урахуванням всіх загрози, що впливають на ресурс):

$$\mathrm{CThR} = 1 - \prod_{i=1}^{n} (1 - \mathrm{CTh}_i), \tag{1.10}$$

Загальний рівень загрози становитиме від 0 до 1.

Розрахуємо ризик по ресурсу R:

$$R = CThR \times D, \quad (1.11)$$

де D – критичність ресурсу (зазначається в грошах або рівнях);

CThR - загальний рівень загроз по ресурсу.

Інформація, з якою працює, і вартість збитку. Вартість інформаційного ресурсу визначалася його власниками.

Задля максимального спрощення моделі знехтуємо втратами від простою устаткування; максимальний збиток інформаційній системі буде дорівнювати вартості інформаційної системи.

Список всіх загроз, що можуть здійснити вплив на інформаційні ресурси, та вірогідність реалізації загроз.

1. Вплив на ресурс:

- неавторизоване проникнення зловмисника всередину об'єкту, за яким здійснюється нагляд (охорона);

- читання цінної інформації з паперових носіїв і екранів персональних комп'ютерів;

- модифікація цінної інформації на паперових носіях;

- видалення чи псування носіїв з цінною інформацією;

- викрадення носіїв з цінною інформацією (паперових носіїв, дискет, компакт-дисків, флеш-карт);

- установка пристроїв зняття електромагнітних коливань;

- отримання конфіденційної інформації без застосування спеціальних засобів (візуальне спостереження, прослуховування).

2. На канал зв'язку:

- пошкодження кабелів;

- несанкціоноване бездротове підключення до кабельної лінії;

- несанкціоноване дротове підключення до кабельної лінії.

3. Загрози «природного» характеру:

- пожежа;

- затоплення;

- удар блискавки;

- неприпустима температура і вологість;

- перепади напруги в електромережі.

4. Загрози, пов'язані з відмовою устаткування:

- втрата даних в результаті відмови їх носіїв;

- дефектні носії інформації;

- закінчення терміну експлуатації обладнання;

- переповнення пристроїв зберігання інформації (в цьому випадку можливі втрати даних).

5. Загрози операційній системі / прикладного програмного забезпечення:

- розширення привілеїв користувача під час реалізації локальних вразливостей, що використовують помилки розробки операційної системи;

- розширення привілеїв користувача під час реалізації локальних вразливостей, що застосовують помилки адміністрування операційної системи (ОС);

- підміна системних конфігураційних файлів / прикладного програмного забезпечення;

- відмова в обслуговуванні ОС.

6. Загрози інформації:

- неавторизована зміна електронних документів / інформації в базі даних;

- неавторизоване читання конфіденційних даних в базі даних / в електронних документах;

- ненавмисне використання конфіденційних даних тощо.

7. Загрози мережних служб:

- відмова в обслуговуванні мережевої служби (внутрішній збій програмного забезпечення);

- підбір аутентифікаційних даних користувача;

- перехоплення інформації, яка надається мережевими службами (листів електронної пошти), користуючись вразливістю протоколів передачі інформації.

8. Атаки на мережеве обладнання:

- неавторизований доступ до мережних пристроїв на програмному рівні;

- відмова в обслуговуванні на програмному рівні;

9. Атаки на протоколи зв'язку:

- перехоплення мережевого трафіку на логічному рівні.

До рівня загрози входить ймовірність реалізації даної загрози (P) та вірогідність того, що реалізація загрози здійснить певний вплив на даний ресурс (ER).

Згідно аналізу існуючих загроз, на прикладі об'єкту захисту зробимо оцінку, наведену в таблиці 1.6.

Таблиця 1.6

Загрози, що впливають на ресурси

ЗАГРОЗА	P,%	ER
1.Влив на ресурс		
Читання цінної інформації з паперових носіїв і екранів персональних комп'ютерів	50	55
Знищення або псування носіїв з цінною інформацією	30	5
Крадіжка носіїв з цінною інформацією (паперових носіїв, компакт-дисків, флеш-карт)	40	5
2.Загрози «природного» характеру		
Стихійні лиха	3	5
Неприпустима температура і вологість	1	10
Вимкнення електрики	10	1
3.Вплив на інформацію		
Неавторизоване читання, зміна, видалення електронних документів / інформації в базі даних	20	55
Навмисне використання співробітниками конфіденційної інформації з метою особистої вигоди	60	75
Вимкнення електрики	10	1
Ненавмисне використання співробітниками конфіденційної інформації	40	65

Продовження таблиці 1.6

4.Вплив на мережеві служби		
Відмова в обслуговуванні мережевої служби (внутрішній збій програмного забезпечення)	35	40
Розширення привілеїв віддаленого користувача при реалізації вразливостей, що використовують помилки розробки або адміністрування мережевих служб	15	50
Підбір автентифікаційних даних користувача	15	60

Сумарна вірогідність реалізації загроз для всіх інформаційних ресурсів (таблиця 1.7).

Таблиця 1.7

Рівень загроз

Ресурс	Загальний рівень загроз по ресурсу
1.Вплив на ресурс	0,31
2.Загрози «природного» характеру	0,004
3.Вплив на інформацію	0,82
4. Вплив на мережеві служби	0,395

Висновки до розділу 1

Таким чином, з вищенаведених таблиць можемо дійти до висновку, що перехоплення конфіденційних даних, в тому числі через соціальні мережі, може призвести до колосальних негативних наслідків як для користувача, так і для підприємства, організації, де працює співробітник. Саме тому актуальним питанням є забезпечення захисту персональних даних в соціальних мережах. Існуючі методи та рекомендації з підвищення захисту персональних даних для соціальних мереж будуть наведені у наступних розділах роботи.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

2.1 Аналіз методів захисту від несанкціонованого доступу як задачі забезпечення інформаційної безпеки

Як вже зазначалося, витік персональних даних став однією з найгостріших проблем останніх років. Тому соціальні мережі постійно вдосконалюють свій функціонал, щоб запобігти несанкціонованому доступу до особистих даних та контенту користувача. Але піклуватися про те, щоб конфіденційною інформацією не скористалися зловмисники, варто не лише соцмережам, а й самим користувачам [15].

Захист персональних даних у соціальних мережах полягає в тому, що особисті дані користувача видаляються з серверів ресурсу, якщо користувач видалив свій обліковий запис. Це одне з основних положень політики конфіденційності багатьох соціальних мереж. Але потрібно пам'ятати, що з метою забезпечення користувачеві можливості відновити свій обліковий запис протягом деякого часу після його видалення, соцмережі зберігають всю інформацію протягом певного терміну. Крім того, дані можуть залишитись у кеші пошукових систем та інших електронних ресурсів.

Найпоширеніша помилка, яку роблять користувачі соціальних мереж і якою активно користуються зловмисники, - використання простого, однакового пароля до всіх облікових записів. Такий пароль дуже легко зламати. Інший спосіб, який не втрачає популярності, незважаючи на численні публікації, що стосуються цієї теми, це так звана соціальна інженерія. Зловмисники моделюють ситуації, що дискомфортні для користувача і вимагають від нього швидкого вирішення. У таких ситуаціях багато людей дають зловмиснику ту інформацію, яка йому потрібна, - номер банківської картки, логін-пароль від облікового запису тощо.

Захист у соціальних мережах – це не в останню чергу критичне ставлення до будь-яких взаємодій, у ході яких зловмисники намагаються якусь інформацію.

Несанкціонований доступ – це навмисне протиправне отримання доступу до сторінки в соціальній мережі і заволодіння конфіденційною інформацією особою, яка не має права доступу до даної інформації. Часті причини несанкціонованого доступу – це слабкі паролі, атаки соціальної інженерії (фішинг), внутрішні загрози, зламування облікових даних, шкідливе ПЗ, спам.

Для забезпечення захисту персональних даних використовуються програмні та криптографічні засоби. Програмні засоби:

- DLP-системи - комплексні системи, що запобігають витоку даних;

- SIEM-системи – комплексні системи управління подіями та інформаційною безпекою, що відстежують у режимі реального часу події безпеки (тривог);

- криптографічні засоби;

- системи автоматизованого тестування.

Розглянемо основні засоби захисту від несанкціонованого доступу.

DLP системи – це набір інструментів і процесів, які використовуються для того, щоб конфіденційні дані не були втрачені, використані не за призначенням або отримали доступ до них неавторизованих користувачів. Програмне забезпечення DLP класифікує дані та виявляє порушення політик, викладених, наприклад, соціальною мережею або в рамках визначеного пакета політик, які зазвичай обумовлені дотриманням нормативних вимог [16-18].

Після виявлення таких порушень DLP застосовує заходи з виправлення із використанням шифрування, попереджень, інших захисних дій. Вони допоможуть не допустити випадковий чи зловмисний обмін даними кінцевими користувачами, який може зазнати організації ризику. ПЗ (програмне забезпечення) та інструменти для запобігання втрати інформації відстежують й контролюють дії кінцевих точок, а також фільтрують потоки даних і відстежують дані.

DLP також надає звіти для відповідності вимогам відповідності та аудиту та виявлення слабких місць та аномалій для експертизи та реагування на ті інциденти, що сталися [19,20].

Поєднання управління інформацією про безпеку (SIM) та управління подіями безпеки (SEM), управління інформацією про безпеку та події (SIEM) забезпечує моніторинг та аналіз подій у режимі реального часу, а також відстеження та реєстрацію даних безпеки для забезпечення відповідності вимогам або аудиту [21].

SIEM — це рішення для забезпечення безпеки, яке допомагає розпізнавати потенційні загрози безпеці та вразливості, перш ніж вони зможуть порушити конфіденційність. Така система виявляє аномалії у поведінці користувачів та використовує штучний інтелект для автоматизації багатьох ручних процесів, пов'язаних з виявленням загроз та реагуванням на інциденти, і є основною у сучасних операційних центрах безпеки (SOC) для сценаріїв використання управління безпекою та відповідністю вимогам.

На самому базовому рівні всі рішення SIEM виконують певний рівень функцій агрегації, консолідації та сортування даних для виявлення загроз та дотримання вимог відповідності даних. Хоча деякі рішення відрізняються за можливостями, більшість із них пропонують однаковий базовий набір функцій [22]:

1. Керування журналом. SIEM збирає дані про події з різних джерел. Журнали та потокові дані збираються, зберігаються та аналізуються в режимі реального часу, що дає можливість автоматично керувати журналом подій в одному централізованому місці.

Деякі рішення SIEM також інтегруються зі сторонніми каналами аналітики загроз, щоб зіставляти їхні внутрішні дані безпеки з раніше розпізнаними сигнатурами та профілями загроз. Інтеграція з потоками загроз у режимі реального часу дозволяє блокувати чи виявляти нові типи сигнатур атак.

2. Кореляція подій та аналітика Кореляція подій є невід'ємною частиною будь-якого рішення SIEM. Використовуючи розширену аналітику для виявлення

та розуміння складних шаблонів даних, кореляція подій дозволяє швидко виявляти та усувати потенційні загрози для безпеки. Рішення SIEM значно покращують середній час виявлення (MTTD) та середній час відповіді (MTTR) за рахунок розвантаження ручних робочих процесів, пов'язаних із поглибленим аналізом подій безпеки.

3. Моніторинг інцидентів та оповіщення безпеки. Оскільки системи забезпечують централізоване управління, рішення SIEM здатні ідентифікувати всі елементи IT-середовища. Це дозволяє технології SIEM відслідковувати інциденти безпеки для всіх підключених користувачів, пристроїв та програм, класифікуючи ненормальну поведінку в міру її виявлення в мережі. Використовуючи певні правила кореляції, адміністратори можуть негайно отримувати оповіщення і вживати відповідних дій для пом'якшення наслідків до того, як вони матеріалізуються в більш серйозні проблеми з безпекою.

4. Управління відповідністю та звітність. Враховуючи, що користувач соціальної мережі може виконувати вхід з корпоративної мережі, рішення SIEM - популярний вибір для організацій, на які поширюються різні форми дотримання нормативних вимог. Завдяки автоматизованому збору та аналізу даних SIEM є цінним інструментом для збору та перевірки даних про відповідність у всій інфраструктурі. Рішення SIEM можуть генерувати в режимі реального часу звіти, знижуючи навантаження на управління безпекою та виявляючи потенційні порушення на ранньому етапі, щоб їх можна було усунути. Багато рішень SIEM поставляються з готовими надбудовами, які можуть генерувати автоматичні звіти, призначені для відповідності вимогам відповідності.

Криптографічні засоби. До такого виду засобів відносяться шифрування інформації, посвідчення входу та дій на сайті та деякі інші інструменти.

Розглянемо декілька видів алгоритмів шифрування, які широко застосовуються в нинішній час. Актуальні наразі схеми шифрування користуються концепцією відкритого й симетричного ключа. Основні відмінності симетричних та асиметричних алгоритмів, які можна застосовувати для шифрування дискретних даних, представлені в таблиці 2.1.

Таблиця 2.1

Основні відмінності симетричних та асиметричних алгоритмів

Критерій порівняння	Симетричне шифрування	Асиметричне шифрування
1. Кількість ключів	Застосовується тільки один ключ (симетричний), а також він же використовується задля шифрування й дешифрування повідомлення.	Два криптографічні ключі, що відрізняються (асиметричні ключі), та називаються відкритим й приватним ключами, застосовуються задля шифрування й дешифрування.
2. Складність та швидкість виконання	Проста техніка, через що процес шифрування здійснюється швидко.	Значно складніший за симетричне шифрування процес, до того ж процес триває довше.
3. Довжина ключів	Довжина застосованих ключів в середньому становить 128 чи 256 біт, в залежності від вимог безпеки.	Ключів значно довші: рекомендований розмір ключа RSA — 2048 біт чи більше.
4. Використання	Використовується зазвичай в разі потреби передати великі об’єми інформації.	Застосовується при невеликих транзакціях — для автентифікації, встановлення безпечного каналу зв'язку.
5. Безпека	Спільний секретний ключ. Це менш захищений процес у порівнянні з асиметричним шифруванням.	Приватний ключ, що не використовується спільно. Загальний процес є безпечнішим, якщо порівнянні з симетричним шифруванням.
6. Приклади алгоритмів	CAST-128, BLOWFISH, IDEA, 3DES, AES, DES, RC2, RC4, RC5, RC6 тощо.	Diffie-Hellman, RSA, ECC та інші.

Розглянемо деякі алгоритми.

Алгоритм CAST-128. CAST-128, також відомий як CAST5, є блоковим шифром, що використовується в ряді продуктів CAST-128 був створений в 1996 році Карлайлом Адамсом і Стаффордом Таваресом.

CAST-128 - це мережа Фейстеля з 12 або 16 циклами з розміром блоку 64 біт та розміром ключа від 40 до 128 біт (але тільки з кроком 8 біт). Якщо розмір

ключа перевищує 80 біт, використовуються повні 16 раундів. Компоненти включають великі 8 x 32-бітові S-блоки, засновані на функціях вигину, які залежні від ключа обертання, модульному складанні і відніманні і операціях XOR. Є три типи раундової функції, але вони схожі за структурою і відрізняються тільки вибором точної операції (складання, віднімання або XOR) у різних точках.

CAST-256, також відомий як CAST6, був отриманий із CAST-128 та опублікований у червні 1998 року. Він був представлений як кандидат на Advanced Encryption Standard (AES). CAST-256 використовує ті ж елементи, що і CAST-128, включаючи S-блоки, але адаптовані для розміру блоку 128 біт - удвічі більше, ніж у 64-бітного попередника. Допустимі розміри ключа: 128, 160, 192, 224 або 256 біт. CAST-256 складається з 48 раундів.

Блок-схема алгоритму представлена на рисунку 2.1.

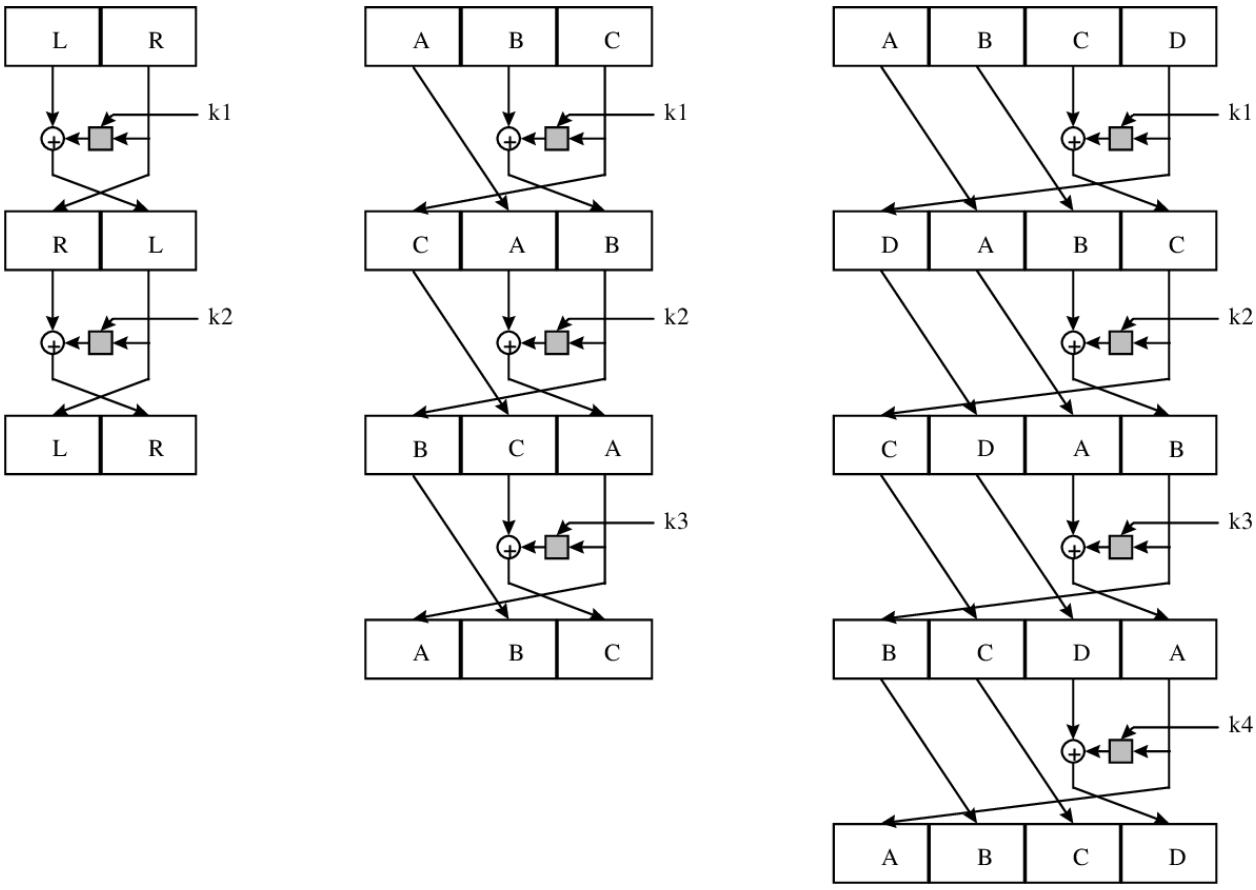


Рисунок 2.1 - Блок-схема алгоритму

Як для шифрування (encrypt()), так і для дешифрування (decrypt()) алгоритм CAST-128 приймає на вхід ключ key і msg, що кодується.

Принцип роботи функцій encrypt() і decrypt() дуже схожий, але є й відмінність: для розшифровки потрібно робити те саме, що й при шифруванні, але у зворотному порядку. Для цього при програмній реалізації необхідно створити допоміжну функцію run(), якою можна передати додатковий прапор reverse (false для шифрування та true для дешифрування).

Передбачається, що шифрування та дешифрування здійснюється "на місці". Тобто, повідомлення msg кодуються без копіювання.

Blowfish. Blowfish – це симетричний блоковий шифр, який можна використовувати як заміну DES або IDEA. Він приймає ключ змінної довжини, від 32 до 448 біт, що робить його ідеальним як для домашнього, так експортного використання. Blowfish був розроблений Брюсом Шнайєром у 1993 році як швидка безкоштовна альтернатива існуючим алгоритмам шифрування. З того часу він зазнав значного аналізу і поступово отримує визнання як надійний алгоритм шифрування. Blowfish не запатентований, не вимагає ліцензії та доступний безкоштовно для будь-якого використання.

При проектуванні Blowfish використовувалися такі критерії [23]:

- Швидкість. Blowfish зашифровує дані на 32-бітових мікропроцесорах із швидкістю 26 тактів на байт.

- Компактність — шифр може займати не більше 5 Кбайт пам'яті.

- Легкість. Шифр користується тільки простими операціями, такими як XOR, додавання, вибірка з таблиці за 32-бітовим операндом. Через те, що проаналізувати його схеми просто, кількість помилок під час реалізації коду зменшується.

- Безпека. Blowfish має змінну довжину ключа, що може сягати 448 бітів.

Blowfish є 64-бітовим блоковим шифром, що має ключ змінної довжини. Його алгоритм містить дві частини: розгортання ключа й шифрування даних. Завдяки розгортанню ключа, ключ з довжиною не більше 448 бітів

перетворюється на декілька масивів підключів, що мають загальний обсяг — 4168 байтів.

Алгоритм шифрування представлений на рисунку 2.2.

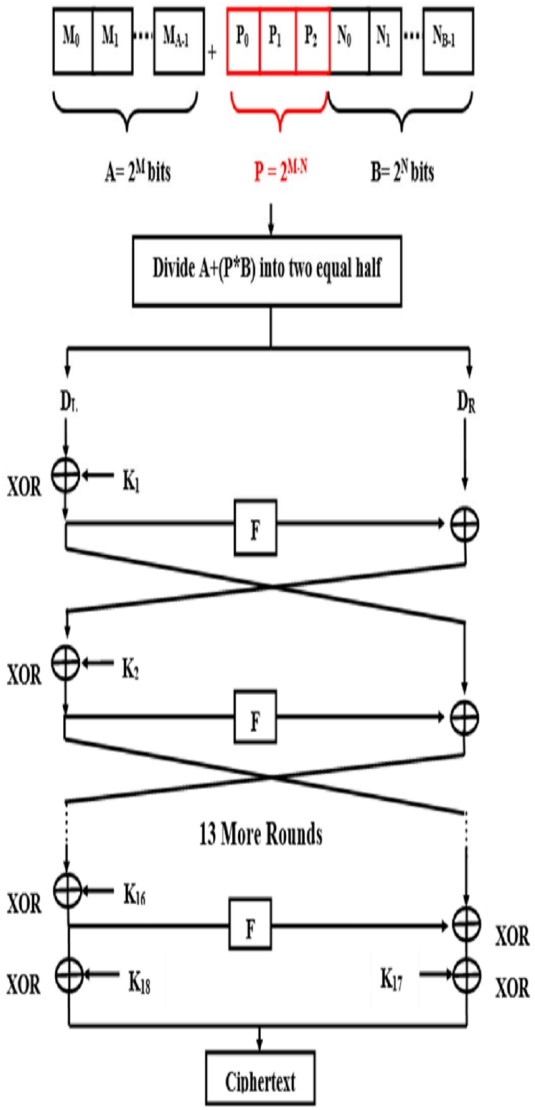


Рисунок 2.2 - Блок-схема алгоритму шифрування Blowfish

Алгоритм шифрування даних (IDEA) – це колись пропрієтарний безкоштовний та відкритий блоковий шифр, який колись призначався для заміни стандарту шифрування даних (DES). Колись званий покращеним пропонованим стандартом шифрування (IPES) IDEA є незначною редакцією стандарту шифрування (PES).

Алгоритм шифрування представлений на рисунку 2.3.

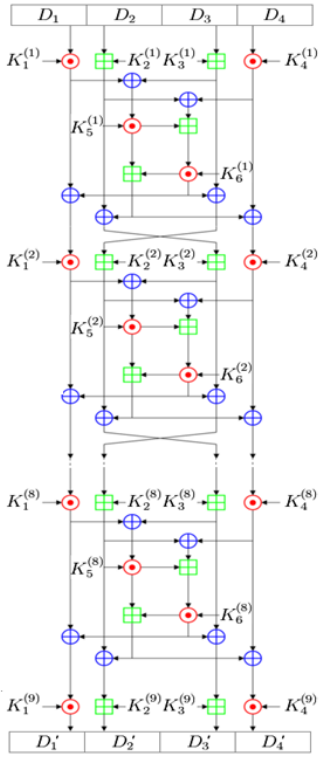


Рисунок 2.3 - Алгоритм шифрування IDEA

IDEA використовує аналогічні процеси для шифрування та дешифрування з деяким зворотним порядком раундових ключів. Алгоритм складається із серії з 8 циклів і працює з 64-бітними блоками з використанням 128-бітного ключа. IDEA «страждала» від слабких ключів до тих пір, поки не було переглянуто її розклад ключів, і в майбутньому може знадобитися подальший перегляд.

Характеристики:

- використовує відкритий текст фіксованої довжини з 16 біт і шифрує їх 4 блоками по 4 біти кожен для створення 16-бітного зашифрованого тексту;

- довжина використовуваного ключа становить 32 біти.

Ключ також поділено на 8 блоків по 4 біти в кожному.

Цей алгоритм включає серію з 4 ідентичних повних раундів та 1 півкола. Кожен повний раунд включає серію з 14 кроків.

Після 4 повних раундів фінальне «півколо» складається лише з перших 4 з 14 кроків, які раніше використовувалися в повних раундах. Для виконання цих циклів кожне двійкове уявлення має бути перетворене на його еквівалентне десяткове уявлення, виконати операцію, і отриманий результат повинен бути

перетворений назад у двійкове уявлення для остаточного результату цього конкретного кроку.

Розклад ключів: 6 підключів по 4 біти із 8 підключів використовуються в кожному повному раунді, а 4 - у півкрузі. Отже, для 4,5 раундів потрібно 28 підключів. Цей ключ, "K", безпосередньо дає перші 8 підключів. Шляхом повороту основного ключа вліво на 6 бітів між кожною групою з 8 створюються додаткові групи з 8 підключів, що має на увазі менше одного повороту за раунд для ключа (3 повороти).

16-бітовий відкритий текст може бути представлений як X1 | X2 | X3 | X4 кожен розміром 4 біта. 32-бітний ключ розбитий на 8 підключів, позначених як K1 | K2 || K3 || K4 || K5 || K6 || K7 || K8, знову розміром 4 біти кожен. У кожному раунді з 14 кроків використовуються три операції алгебри: додавання по модулю (2 ^ 4), множення по модулю (2 ^ 4) +1 і побітове виключення.

Алгоритм RC5 розроблений найвідомішим криптологом Рональдом Рівестом – одним із розробників асиметричної системи RSA. Як і попередні аналогічні алгоритми шифрування Рона Рівеста RC2 та RC4 (є потоковим шифром), алгоритм RC5 знайшов дуже широке поширення.

На перетвореннях, що застосовуються в RC5, було засновано подальшу розробку компанії RSA. Алгоритм RC6 став фіналістом конкурсу AES щодо вибору нового стандарту шифрування в Сполучених Штатах Америки [24].

Деякі з головних параметрів алгоритму RC5 змінні. Окрім секретного ключа, до параметрів алгоритму відносяться:

- розмір слова w (у бітах); RC5 блоками шифрує два окремих набори дискретних даних; допустимі значення w — 16, 32 чи 64, рекомендованим з яких є 32;

- число раундів алгоритму R – в якості значення допускається будь-яке ціле число (0-255 включно);

- розмір секретного ключа b – будь-яке значення в байтах (0-255 включно).

Задля уточнення параметрів алгоритму найчастіше застосовується позначення RC5-w/R/b. Приклад: RC5-32/12/16 позначає RC5 із 64-бітним блоком, 12 раундами й 128-бітним (16-байтним) ключем.

Змінні параметри дозволяють розширити сферу використання даного алгоритму та значно скорочують витрати у разі необхідності переходу на більш сильний варіант алгоритму, програмної чи апаратної реалізації алгоритму, що підтримує змінні параметри. Усунути проблему нескладно, замінивши ключ довшим.

Автором в алгоритмі передбачена проблема сумісності реалізацій RC5 з різними параметрами. Перед кожним зашифрованим повідомленням радиться ставити заголовок, який містить список значень основних параметрів алгоритму. В цьому випадку для розшифровування повідомлення необхідно встановити параметри із заголовка, після чого в разі введення коректного ключа повідомлення буде з легкістю розшифровано.

Структура алгоритму RC5 наведена на рисунку 2.4.

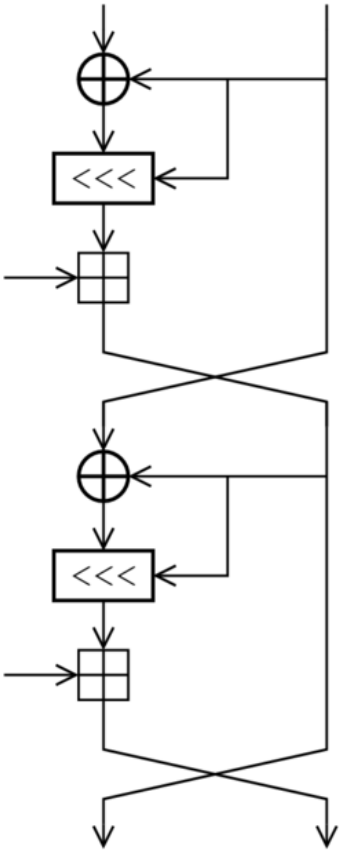


Рисунок 2.4 - Структура алгоритму RC5

Алгоритм є мережею Фейстеля, у кожному раунді якої виконуються такі операції:

$$A = \big((A \oplus B) \ll B\big) + K_{2*r} \; mod \; 2^w, \tag{2.1}$$

$$B = \big((A \oplus B) \ll A\big) + K_{2*r+1} \; mod \; 2^w, \tag{2.2}$$

де r – номер поточного раунду, починаючи з 1,

K_n - фрагмент розширеного ключа,

$\ll n$ - Операція циклічного зсуву на x бітів вліво, де x - значення молодших $log_2 w$ бітів n.

Перед першим раундом виконуються операції накладання двох перших фрагментів розширеного ключа на дані, що шифруються:

$$\mathrm{A} = \mathrm{A} + \mathrm{K_0} \bmod 2^{\mathrm{w}}, \tag{2.3}$$

$$\mathrm{B} = \mathrm{B} + \mathrm{K_1} \bmod 2^{\mathrm{w}}. \tag{2.4}$$

Під словом «раунд» в описі алгоритму розуміються перетворення, що відповідають двом раундам звичайних алгоритмів, структура яких мережа Фейстеля.

Тобто раунд алгоритму RC5 обробляє блок повністю, тоді як типовий раунд мережі Фейстеля обробляє лише один субблок – зазвичай половину блоку.

Алгоритм простий – у ньому використовуються тільки операції додавання по модулю 2 і 2^w по модулю, а також зрушення на змінну кількість бітів. Зрушення на змінну кількість бітів є дуже просто реалізованою операцією, яка, проте, істотно ускладнює лінійний та диференціальний криптоаналіз алгоритму. Простий алгоритм реалізувати та аналізувати щодо можливих уразливостей легше — дана простота алгоритму є його важливою перевагою [25].

Розшифровування виконується застосуванням зворотних операцій на зворотній послідовності, тобто, у всіх раундах r (із зворотною послідовністю раундів) спостерігаються такі операції:

$$B = ((B - K_{2*r+1} \bmod 2^w) \gg A) \oplus A, \quad (2.5)$$

$$A = ((A - K_{2*r} \bmod 2^w) \gg B) \oplus B, \quad (2.6)$$

де »n - аналогічна описаній вище («n) операція побітового циклічного зсуву вправо.

Відповідно, після R раундів виконуються такі операції:

$$B = B - K_1 mod\ 2^w, \quad (2.7)$$

$$A = A - K_0\ mod\ 2^w. \quad (2.8)$$

Алгоритм RC5 та деякі його варіанти є запатентованими.

ECC. Це алгоритм асиметричного шифрування нового покоління. Його застосовують також при створенні ключів шифрування і створенні безпечних з'єднань задля безпечної передачі інформації. ECC набагато безпечніше й швидше RSA чи DSA, використовує ключі, що коротші, ніж RSA, які до того ж складно зламати. 512-бітовий ECC ключ безпечний настільки ж, як і 15360-бітний ключ RSA, проте через його менші розміри він споживає значно менше обчислювальної потужності для його генерації. Використовується ECC не настільки ж часто, як RSA, адже це відносно новий алгоритм. Окрім того, RSA реалізувати легше [26].

Еліптична крива криптографії (ECC) існує з середини 1980-х років, але вона, як і раніше, розглядається як новачок у світі SSL і тільки почала отримувати визнання за останні кілька років. ECC - принципово інший математичний підхід до шифрування, ніж алгоритм RSA. Еліптична крива є функцією алгебри ($y^2 = x^3 + ax + b$), яка виглядає як симетрична крива, паралельна осі x при побудові графіка.

Алгоритм шифрування наведений на рисунку 2.25.

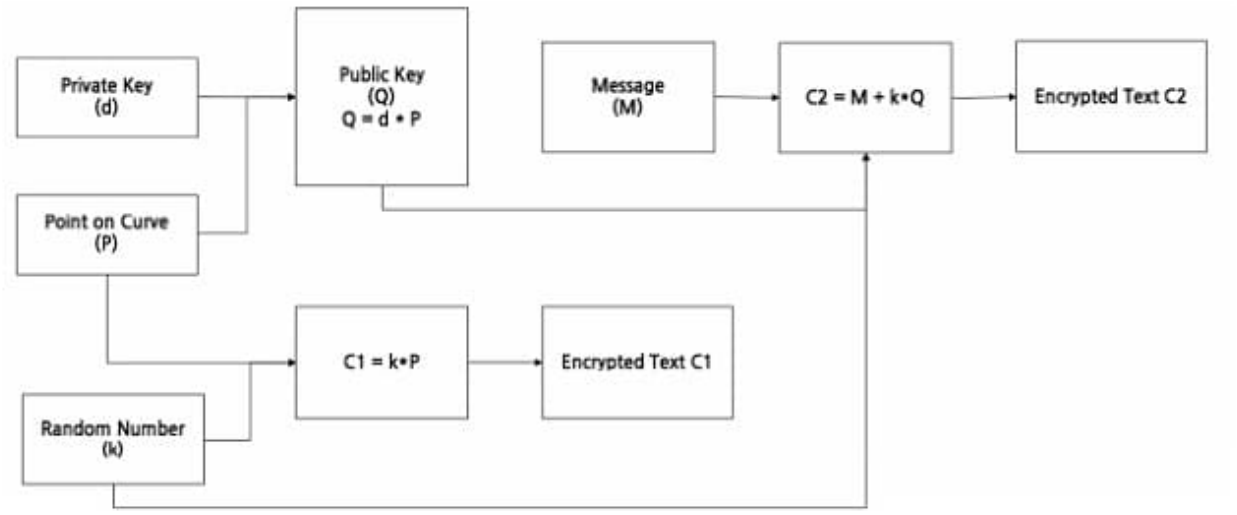


Рисунок 2.5 - Алгоритм шифрування ECC

Як і в інших формах криптографії з відкритим ключем, ECC заснований на односторонній властивості, в якій легко виконати обчислення, але система не піддається зворотному результату розрахунку, щоб знайти вихідні числа. Для досягнення цієї властивості ECC використовує інші математичні операції, ніж RSA. Найпростіший спосіб пояснити цю математику - для еліптичної кривої лінія проходитиме тільки через три точки вздовж кривої (P, Q і R) і що, знаючи дві з точок (P і Q), інша (R) можна легко обчислити, але тільки з R, дві інші, P і Q, не можуть бути отримані.

ECC використовується як у цифрових підписах за допомогою еліптичної кривої DSA (ECDSA), так і при обміні ключами через Elliptic Curve Diffie-Hellman (ECDH).

Ці алгоритми застосовуються у різних частинах стандарту SSL. По-перше, сертифікати SSL можуть бути підписані з ECDSA замість RSA. Друге використання для ECC, коли сервер та клієнт узгоджують ключі сеансу, які використовуються для шифрування всіх даних, що надсилаються між сервером та браузером. У цьому останньому випадку сервер та браузер мають бути налаштовані для підтримки наборів шифрування ECDH.

Головною перевагою ECC є те, що він сильніший за RSA для ключових розмірів, що використовуються сьогодні.

Щоб випередити обчислювальну потужність зловмисника, ключі RSA повинні бути довшими.

Іншою перевагою ECC у плані безпеки є просте надання альтернативи RSA та DSA. Якщо виявлено серйозну слабкість RSA, ECC, ймовірно, стане кращою альтернативою, особливо якщо раптова слабкість RSA вимагає різкого збільшення розміру ключа для компенсації [27].

ECC також швидше з низки причин. По-перше, менші ключі означають менше даних, які мають бути передані із сервера клієнту під час встановлення зв'язку SSL. Крім того, ECC вимагає менше обчислювальної потужності (ЦП) та пам'яті, що призводить до значного збільшення часу відгуку та пропускної спроможності на веб-серверах, коли вони використовуються.

Системи автоматизованого тестування. Система автоматизованого тестування може сканувати, в тому числі і мережі, на предмет великої кількості варіантів уразливостей за декілька годин. І, на відміну від людини, автоматичний сканер безпеки не може забути просканувати вхідний параметр.

Виконуючи ручний тест безпеки, виникає обмеження проникнення рядом відомих уразливостей, відомих тестеру на проникнення. З іншого боку, при використанні автоматичного сканера, можливо переконатися, що всі параметри перевіряються на відповідність усім типам варіантів безпеки.

Використовуючи системи автоматизованого захисту, можна гарантувати, що в результатах сканування безпеки не буде повідомлень про помилкові спрацьовування, тому не потрібно виділяти час на перевірку виявлених уразливостей.

2.2 Модульний алгоритм захисту від несанкціонованого доступу

У ході аналізу існуючих методів захисту від несанкціонованого доступу доцільно зробити алгоритм модульним, це дозволить в залежності від поставленого завдання модульно конструювати алгоритм для систем, яким необхідний підвищений рівень безпеки.

Модулі алгоритму захисту наведені у вигляді таблиці 2.2.

Таблиця 2.2

Модулі алгоритму захисту від несанкціонованого доступу

Методи	Потрібні для більшості проектів	Використовується в системах з підвищеним рівнем безпеки
Перевірка IP на наявність у чорному списку	+	+
Перевірка IP на наявність у публічних чорних списках	+	+
Перевірка User-Agent браузера	+	+
Підтвердження входу через e-mail	+	+
Капча – перевірка	+	+
Обмеження за кількістю запитів	+	+
Поля приманки	+	+
Побудова форми за допомогою JavaScript	+	+
Обмеження за часом заповнення та відправлення форми	+	+
Перевірка правильності заповнення веб-форм	+	+
Верифікація особи по кредитній картці	-	+
Зміна імен полів веб-форм	-	+
Підтвердження входу за допомогою SMS-сповіщення	-	+

Модулі, які наведені у вигляді таблиці 2.2, дозволяють підвищити захищеність соціальної мережі. Мережа здатна обмежувати кількість запитів та намагатися відрізнити людини від робота за другорядними ознаками у поведінці. Непрямі ознаки не дають гарантії, лише збільшують ймовірність те, що зловмисник «не пройде».

Також задачею є захист соціальної мережі від спаму. Головною відмінністю бота від людини є бачення сторінки у соцмережі в якості послідовності тексту й тегів, в той час як для людини важливим є візуальний образ, тобто кінцевий результат, а не власне код сторінки.

Наприклад, у формах реєстрації роблять невидимі для користувача поля з розрахунком на те, що бот, аналізуючи не зовнішній вигляд сторінки, а її HTML-код, ці поля заповнить і цим видасть себе.

Більшість методів, що не вимагають активних дій від користувача під час відправки Web-форми, засновані на тому, що середньостатистичний бот, не навчений інтерпретувати JavaScript, CSS, Flash і т.д. на відміну від повноцінного браузера.

Однак непрямі методи визначення менш ефективні, ніж CAPTCHA, тому переважна більшість соціальних мереж, що борються з використанням їх сервісів

ботами, використовує CAPTCHA-завдання, бо непрямі способи захисту розраховані те, що бот тим чи іншим чином проявить свою сутність, а чи не те що, щоб поставити перед ботом принципово складне йому завдання.

Обмеження кількості запитів з однієї IP-адреси – це досить простий спосіб, проте малоефективний за достатньої підготовленості атакуючого. Можна робити запити через анонімні проксі, внаслідок чого сайт бачить IP-адресу відвідувача адресу проксі. Зловмисник може використовувати велику кількість проксі-серверів. Обмеження через виставку відвідувачеві cookie також є малоефективним, їх легко можна стерти або зовсім ігнорувати.

Обмеження кількості запитів від одного користувача має сенс, коли захищається соціальна мережа, на якій зловмиснику вигідно робити багато запитів, наприклад, при розсилці спаму.

Блокування за часом, заповнення та надсилання форми. Також захищає тип блокування, що відбувається під час обробки повідомлень за певний період часу, що відповідає терміну між завантаженням форми і її відправкою, адже людина виконує цю задачу не так швидко, як робот (йому вистачає 1-2 сек).

Зміна імен полів, що використовуються для передачі даних. Основна маса спам-ботів шукають певні поля на сторінках, що мають стандартні імена («name», «email» тощо. Щоб ускладнити процес автоматичного заповнення цих форм, можна дати полям нестандартні назви, а саме: для поля «електронна пошта» присвоїти ім’я «name», а для поля «ім'я» – «mail».

Створення полів-приманок. Через те, що спам-робот має знайти поля «email», «name» чи інші, йому можна створити приховане засобами CSS поле (не hidden). Рядовий відвідувач таке поле не побачить та не заповнить його на відміну від спам-боту. Форма має оброблятись лише, якщо приховане поле порожнє. Поруч із полями-приманками зазвичай мають бути присутніми поля, що може побачити користувач, та все ж їм необхідно задати нестандартні імена.

Блокування за даними, що віддається браузером.

Цей спосіб захисту реалізується за не складної схемою: у ситуації, коли при програмному визначенні у користувача немає розмірів екрана, інформації про

його браузер, робиться висновок, що форму намагається відіслати бот, і через це її обробляти не потрібно.

Побудова форми за допомогою JavaScript. Завдяки цьому методу можливе більш складне аналізування форми: боту потрібно знайти й обробити код JavaScript, лише тоді він зможе побачите потрібне поле. Використання JavaScript є абсолютно прозорим для користувача, виконується у фоновому режимі і ніяк не відбивається на дизайні сторінки соціальної мережі. Наразі соціальні мережі майже не обходяться без використання JavaScript у своєму основному функціоналі.

Розглянемо основні засоби захисту форм від спаму за допомогою JavaScript. Перший надійніший, але більш громіздкий, полягає у малюванні через document.write всієї форми цілком. При грамотному використанні цього способу спам-бот навіть не знатимуть про наявність форми в соціальній мережі. Мінус у тому, що цей спосіб підходить лише для невеликих форм з кількох полів і не завжди може бути використаний у шаблонних сайтах.

Приклад форми першого способу захисту представлений на рисунку 2.6.

Code (JavaScript):

```
1.  <script type="text/javascript">
2.  document.write('<fo' + 'rm action="gue' + 'st.php?add=1" met' + 'hod="post">');
3.  document.write('Ім'я: <inp' + 'ut type"te' + 'xt" name="user' + 'name"><br>');
4.  document.write('Повідомлення:<br><text' + 'area name="mes' + 'sage" cols="20"
rows="10">');
5.  document.write('<\/tex' + 'tarea>');
6.  document.write('<br><in' + 'put type="sub' + 'mit" value=" Надіслати ">');
7.  document.write('<\/fo' + 'rm>');
8.  </script>
```

Рисунок 2.6 - Приклад форми

Другий спосіб полягає в тому, що у формі є певне секретне поле з встановленим значенням. При відображенні сторінки соціальної мережі або надсиланні форми його значення замінюється на інше. Якщо обробнику форми

приходять дані з початковим значенням секретного поля, вони просто ігноруються. Приклад форми другого способу захисту наведено на рисунку 2.7.

```
<form action="guest.php?add=1" method="post" onsubmit="return false;">
 <input type="hidden" name="username"><br>
 Ім'я:<input type="text" name="username"><br>
 Повідомлення:<br>
 <textarea name ="message" cols="20" rows="10"></textarea><br>
 <input type="button" value="Надіслати" onclick="do_submit(this.form);">
</form>
```

Рисунок 2.7 – Приклад форми другого способу захисту

Наприклад, можна призначити скрипт заміни значення кнопку відправки форми. Також можна додати до нього інші корисні дії, наприклад перевірку заповнення імені користувача. Скрипт заміни наведений на рисунку 2.8.

Code (JavaScript in HTML):

```
1.  <script type="text/javascript">
2.  function do_submit(form) {
3.  //Корисне навантаження - перевірка заповнення імені користувача
4.  if (form.username.value=="") {
5.    alert('Введіть ім'я користувача');
6.  }
7.  else {
8.    //Встановіть правильне значення секретного поля
9.    form.nospam.value="OK";
10.    //Надіслати форму
11.    form.submit();
12.  }
13. }
14. </script>
15. <form action="guest.php?add=1" method="post" onsubmit="return false;">
16.  <input type="hidden" name="username"><br>
17.  Ім'я:<input type="text" name="username"><br>
18.  Повідомлення:<br>
19.  <textarea name ="message" cols="20" rows="10"></textarea><br>
20.  <input type="button" value="Надіслати" onclick="do_submit(this.form);">
21. </form>
```

Рисунок 2.8 – Скрипт заміни

Можна ще ускладнити систему захисту третім способом. Він схожий на другий, але замінюється не значення поля, а адреса обробника форми при відправці.

2.3 Двофакторна автентифікація

Деякі соціальні мережі для покращення захисту особистої інформації своїх користувачів запровадили двофакторну автентифікацію. Вона передбачає двоетапний вхід у свій особистий обліковий запис. Перший етап - традиційний - вхід з допомогою логіну та паролю. Другий етап користувач може вибрати за своїм бажанням із трьох варіантів. Перший - унікальний код за смс, другий - унікальний список кодів, які діють лише один раз. Третій метод полягає у використанні спеціальних мобільних додатків, що генерують коди. Наприклад, можна використовувати Google Authenticator. Для нього необхідно сканувати спеціальний QR-код з мобільного пристрою та ввести спеціальний код підтвердження [28].

Крім цього може використовуватися токен – компактний пристрій, призначений для того, щоб забезпечити інформаційну безпеку користувача. Він використовується для ідентифікації свого власника та можливості надання захищеного віддаленого доступу до різних типів інформації. Токен є власністю користувача. Найбільш прості токени не потребують фізичного підключення до комп'ютера. На дисплеї відображається число, що користувач вводить у систему задля здійснення авторизації. Складніші токени під’єднуються до комп'ютера через USB або Bluetooth-інтерфейси. Все це може допомогти захистити особисту інформацію від недоброзичливців та убезпечити сторінку від зломів.

Висновки до розділу 2

Серед ефективних засобів захисту соціальних мереж від несанкціонованого доступу можна виділити наступні:

- застосування DLP-систем;

- застосування SIEM-систем;

- криптографічні засоби; захисту;

- застосування систем автоматизованого тестування;

- застосування двофакторної автентифікації;

- застосування модульного алгоритму захисту від несанкціонованого доступу.

Таким чином, після аналізу методів захисту від несанкціонованого доступу, де було розглянуто програмні та криптографічні засоби та після побудови модульного алгоритму для захисту персональних даних, можна приступати к розробці рекомендацій щодо захисту конфіденційних даних в соціальних мережах.

РОЗДІЛ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ З ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ СОЦІАЛЬНОЇ МЕРЕЖІ

3.1 Розробка політики безпеки

В межах даного розділу розглянемо політику безпеки соціальної мережі з точки зору засобів захисту персональних даних і інформації користувачів.

1. Цілі обробки інформації

Адміністрація Соціальної мережі здійснює обробку інформації про Користувачів, у тому числі їх персональні дані(ПД), з метою виконання зобов'язань Адміністрації Соціальної мережі перед Користувачами щодо використання Соціальної мережі та його сервісів.

2. Склад інформації про користувачів

2.1 ПД Користувачів. ПД Користувачів включають:

2.1.1. Такі дані, що надаються Користувачами для реєстрації в Соціальній мережі: ім'я, прізвище, стать, дата народження, номер мобільного телефону та/або адреса електронної пошти.

2.1.2. Такі дані, що надаються Користувачами з використанням розділу редагування своїх сторінок (у тому числі сімейний стан, дата народження, рідне місто, родинні зв'язки, домашня адреса, інформація про освіту).

2.1.3. Додатково надаються Користувачами на запит Адміністрації Соціальної мережі з метою виконання Адміністрацією зобов'язань перед Користувачами, що випливають із договору на надання Послуг Соціальної мережі. Адміністрація Сайту має право, зокрема, запросити у Користувача копію документа, що посвідчує особу, або іншого документа, що містить ім'я, прізвище, фотографію Користувача, а також іншу додаткову інформацію, яка, на розсуд Адміністрації Соціальної мережі, буде необхідною та достатньою для

ідентифікації такого Користувача та дозволить виключити зловживання та порушення прав третіх осіб.

2.2. Інша інформація про Користувачів, що обробляється Адміністрацією Соціальної мережі. Адміністрація Соціальної мережі може також обробляти іншу інформацію про Користувачів, яка включає:

2.2.1. Додаткові дані, що отримуються при доступі до Соціальної мережі, що включають дані про технічні засоби (пристрої), технологічну взаємодію з Соціальною мережею (в т.ч. IP-адресу хоста, вид операційної системи користувача, тип браузера, географічне положення, постачальник послуг Інтернету, дані з адресної книги, дані, отримані в результаті доступу до камери, мікрофону тощо пристроїв), та наступні дії Користувача Соціальної мережі. Інформація, що автоматично отримується при доступі до Соціальної мережі з використанням закладок (cookies).

2.2.2. Інформація, створювана користувачами в Соціальній мережі поза розділом редагування сторінок.

2.2.3. Інформація, отримана в результаті дій Користувача в Соціальній мережі (зокрема, інформація про вступ до групи / вихід з групи, додавання інших Користувачів до списку друзів, розміщення фотографій, взяття участі / відмови від участі у зустрічах, додавання відеозаписів).

2.2.4.Інформація, отримана внаслідок дій інших користувачів в Соціальній мережі (зокрема, позначки, зроблені на відеозаписах та фотографіях іншими Користувачами).

3. Обробка інформації про користувачів.

3.1. Обробка персональних даних складається з основних принципів:

а) законності цілей та способів обробки персональних даних;

б) сумлінності;

в) відповідності цілей обробки персональних даних цілям, заздалегідь визначеним та заявленим при зборі персональних даних, а також повноваженням Адміністрації Соціальної мережі;

г) відповідності обсягу та характеру оброблюваних персональних даних, способів обробки персональних даних цілям обробки персональних даних;

д) неприпустимість об'єднання створених для несумісних між собою цілей баз даних, що містять ПД.

3.2. Збір персональних даних Користувача здійснюється в Соціальній мережі під час реєстрації, а також надалі при внесенні користувачем за власною ініціативою додаткових відомостей про себе за допомогою інструментарію в Соціальної мережі.

3.3. ПД Користувачів зберігаються виключно на електронних носіях та обробляються з використанням автоматизованих систем, за винятком випадків, коли неавтоматизована обробка персональних даних необхідна згідно з дотриманням вимог законодавства.

3.4. ПД Користувачів не передаються жодним іншим третім особам, за винятком випадків, прямо передбачених Правилами. При вказівці Користувача або за наявності згоди Користувача можлива передача персональних даних інформації, зокрема при використанні додатків.

Для забезпечення реалізації зазначених цілей Користувач погоджується на здійснення Адміністрацією Соціальної мережі з дотриманням застосовного законодавства сервісних розсилок на його адресу (у тому числі опитувань) з метою отримання зворотного зв'язку за допомогою сервісів Адміністрації Соціальної мережі та/або сервісів третіх осіб: електронних повідомлень, SMS та інших видів розсилок , - а також збору, зберігання, накопичення, систематизації, вилучення, зіставлення, використання, наповнення (уточнення) їх даних, а також на отримання та передачу афілійованим особам та партнерам результатів автоматизованої обробки таких даних із застосуванням різних моделей оцінки інформації у вигляді цілісних та/або текстових значень та ідентифікаторів, що відповідають заданим у запитах оціночним критеріям, для обробки даних Адміністрацією Соціальної мережі та/або особами, зазначеними в цьому пункті.

3.5. обставини, при яких знищуються персональні дані:

- самостійне видалення Користувачем інформації зі сторінки;

- самостійне видалення Користувачем власне своєї персональної сторінки в цілому, використовуючи функцію «видалити свою сторінку».

Якщо персональна сторінка була видалена, Адміністрацією Соціальної мережі зберігається на власних електронних носіях внесені Користувачем дані напротязі мінімального терміну, що закріплено чинним законодавством України. При самостійному видаленні своєї сторінки Користувач матиме змогу відновити її напротязі 210 днів із моменту власне видалення персональної сторінки.

3.6. При розміщенні персональної та іншої інформації на своїй сторінці Користувач усвідомлює та за замовчуванням погоджується з тим, що вона може бути доступною для інших користувачів у Інтернеті. Користувач має змогу власноруч визначати режим конфіденційності, а також умови доступу інших користувачів до власної інформації. Адміністрація Соціальної мережі вживає технічних та організаційних заходів задля забезпечення справної роботи відповідного за це інструментарію мережі.

4. Заходи захисту персональної інформації Користувачів

4.1. Адміністрація Соціальної мережі застосовує різноманітні технічні й організаційно-правові заходи задля забезпечення захисту персональних даних Користувачів мережі від неправомірного чи випадкового доступу, знищення, блокування, зміни, копіювання та інших злочинних дій.

4.2. Для реєстрації Користувача у Соціальній мережі застосовується модульний алгоритм захисту від несанкціонованої реєстрації.

4.3. Щоби авторизуватися у Соціальної мережі, необхідно використовувати логін (адреса електронної пошти чи номер телефону). За збереження даної інформації цілком повну відповідальність несе сам Користувач. Він також не має права надавати свій логін і пароль стороннім особам та має вживати заходи задля забезпечення їх конфіденційності.

4.4. Для забезпечення більш надійного захисту інформації про Користувачів Адміністрація Соціальної мережі запровадила двофакторну автентифікацію. Вона передбачає двоетапний вхід у свій особистий обліковий запис. Перший етап - - вхід з допомогою логіну та паролю. Другий етап обирається вибірково серед

трьох різних варіантів. Перший – унікальний код за смс, другий – унікальний список кодів, які діють лише один раз. Третій метод полягає у використанні Google Authenticator, що генерують коди. Для реалізації даної системи Користувачем Адміністрації Соціальної мережі має бути наданий номер власного мобільного телефону.

Задля мінімізації вірогідності використання сторонніми особами логінів і паролів Користувачів з метою розповсюдження спаму від їх адреси, в ситуації, коли Користувач вводить пароль чи логін із застосуванням незвичного для нього сервера (наприклад, сервера іншої держави), * Адміністрація Соціальної мережі перешкоджає входу на персональну сторінку Користувача та використовує відсилання повідомлення із проханням ввести певні цифри номеру телефону Користувача. Якщо мали місце три невдалі спроби при їх введенні можливість авторизації з використанням поточного сервера буде заблокований на 8 годин.

Адміністрація Соціальної мережі також має право на цілі реєстрації та авторизації Користувача. Він може потребувати підтвердити актуальність закріпленого до сторінки задля (верифікацію) телефонного номера, відновлення доступу до власної сторінки може здійснюватися через перевірочний дзвінок-скидання на телефонний номер Користувача, після чого необхідно ввести код – кілька останніх цифр номера, з якого здійснено дзвінок-скидання у відповідному вікні. Залежно від операційної системи мобільного пристрою введення коду у відповідному вікні може здійснюватися автоматично, але лише після отримання дозволу на доступ до історії дзвінків на мобільному пристрої. Дана роздільна здатність надається за допомогою кнопки «Дозволити» або аналогічною.

4.5. У користувача є право отримувати інформацію щодо того, коли саме та з яких саме пристроїв відбувалася авторизація, вхід у його персональну сторінку. Це можна перевірити, перейшовши по посиланню «Показати історію активності», що знаходиться в розділі «Мої Налаштування / Безпека».

3.2 Рекомендації з впровадження механізмів захисту від несанкціонованої реєстрації

Пропонується механізм шифрування даних задля підвищення захисту персональних даних. Розглянемо даний алгоритм шифрування.

Вважається, що ПД мають структуру:

$$A_0, \dots A_n, \tag{3.1}$$

де A_0,..., A_n - байти (n>0).

При цьому виконане припущення:

1. Якщо B - байт, то N(B) - вміст байта у двійковій системі числення, що інтерпретується як ціле число (без знака).

2. rest(i,j) - залишок від розподілу цілого числа (без знака) i на натуральне j.

По визначенню:

$$rest(m, 0) = m, rest(m, 1) = 0, \tag{3.2}$$

для будь-якого значення m.

3. S_0, S_q – ключове слово, що складається з q+1 байтів S_0, ..., S_q (q>0),

4. Знак «*» - побітове додавання за модулем 2.

5. Послідовність C_0 ... C_q C_{q+1} ... C_{q+n+1} – це S_0...S_q A_0...A_n.

Розглянемо безпосередньо шифрування дискретних даних.

А) Пряма формула кодування.

(1) Початковий крок:

for i=0 to q step 1 do (C_i:=S_i);

for i=0 до n Step 1 do (C_{i+q+1}:=A_i);

r:=q+1; m=rest(N(C_{r-1}),r); C_r: = C_r * C_m;

(2) r:=r+1; if r >q+n+1 then STOP;

m:=rest(N(C_{r-1}),r);

C_r: = C_r * C_{r-1} * C_m; goto (2);

Останнє можна переписати у вигляді:

C_r := A_{r-q-1}*C_{r-1}*C_m; goto (2);)

Послідовність, C_{q+1} ... C_{q+n+1} яка отримана після STOP – результат кодування.

Б) Зворотна формула кодування.

Для зворотної формули кодування припустимо, що C_0 ... C_{q+n+1} - послідовність байтів, що надходить. При цьому вважається що послідовність C_0 ... C_q відома і відомий ключ S_0 ... S_q). При цьому A_0 ... A_n - вихідна послідовність байтів.

Нижче наведений алгоритм декодування.

(1) Початковий крок:

r:=q+1; m=rest(N(C_{r-1}),r); A_{r-q-1} = C_r * C_m;

(2) r:=r+1; if r >q+n+1 then STOP;

m:=rest(N(C_{r-1}),r);

C_r: = C_r * C_{r-1} * C_m; goto (2);

Останнє можна переписати у вигляді:

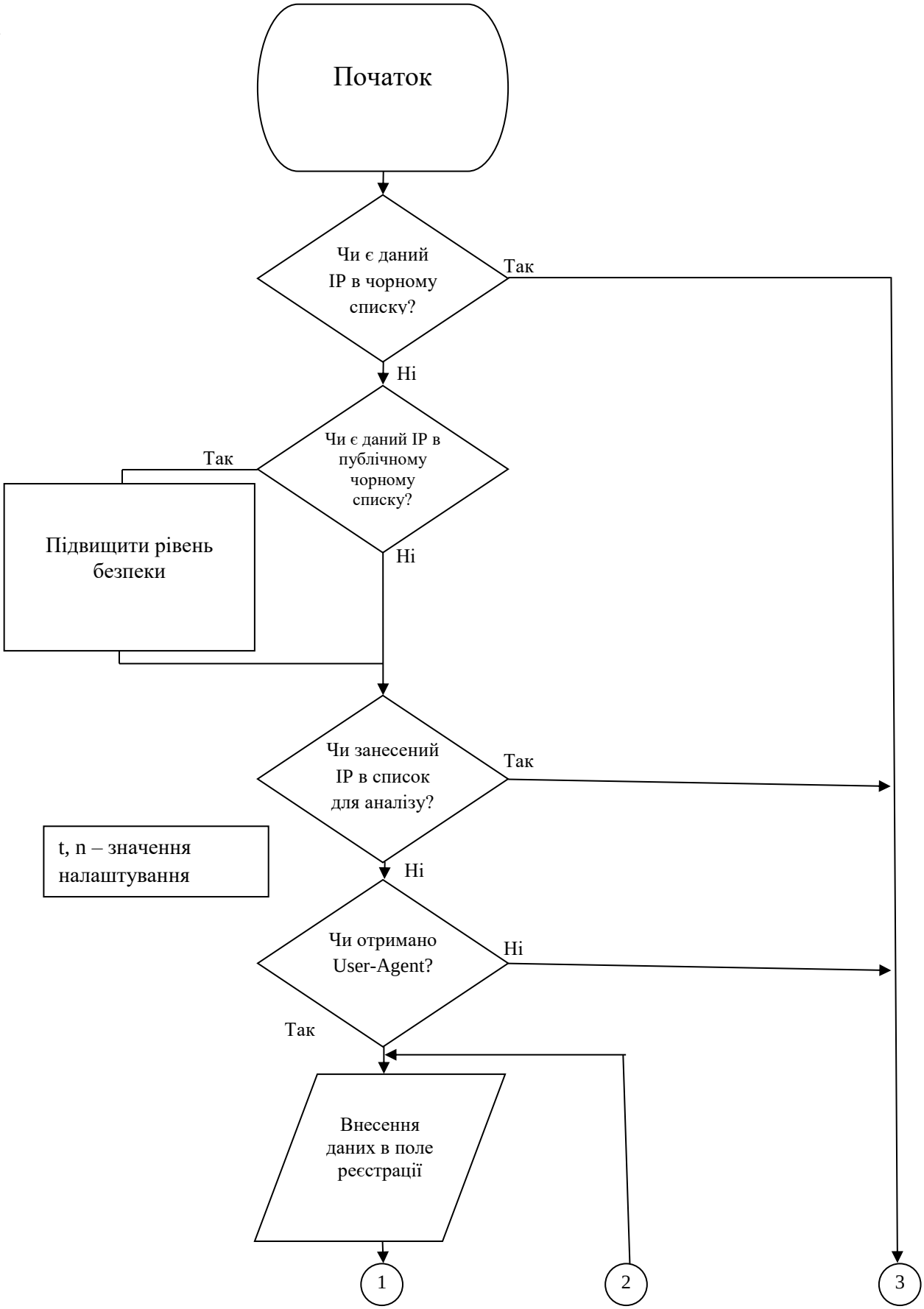
A_{r-q-1}: = C_r * C_{r-1} * C_m; goto (2);)

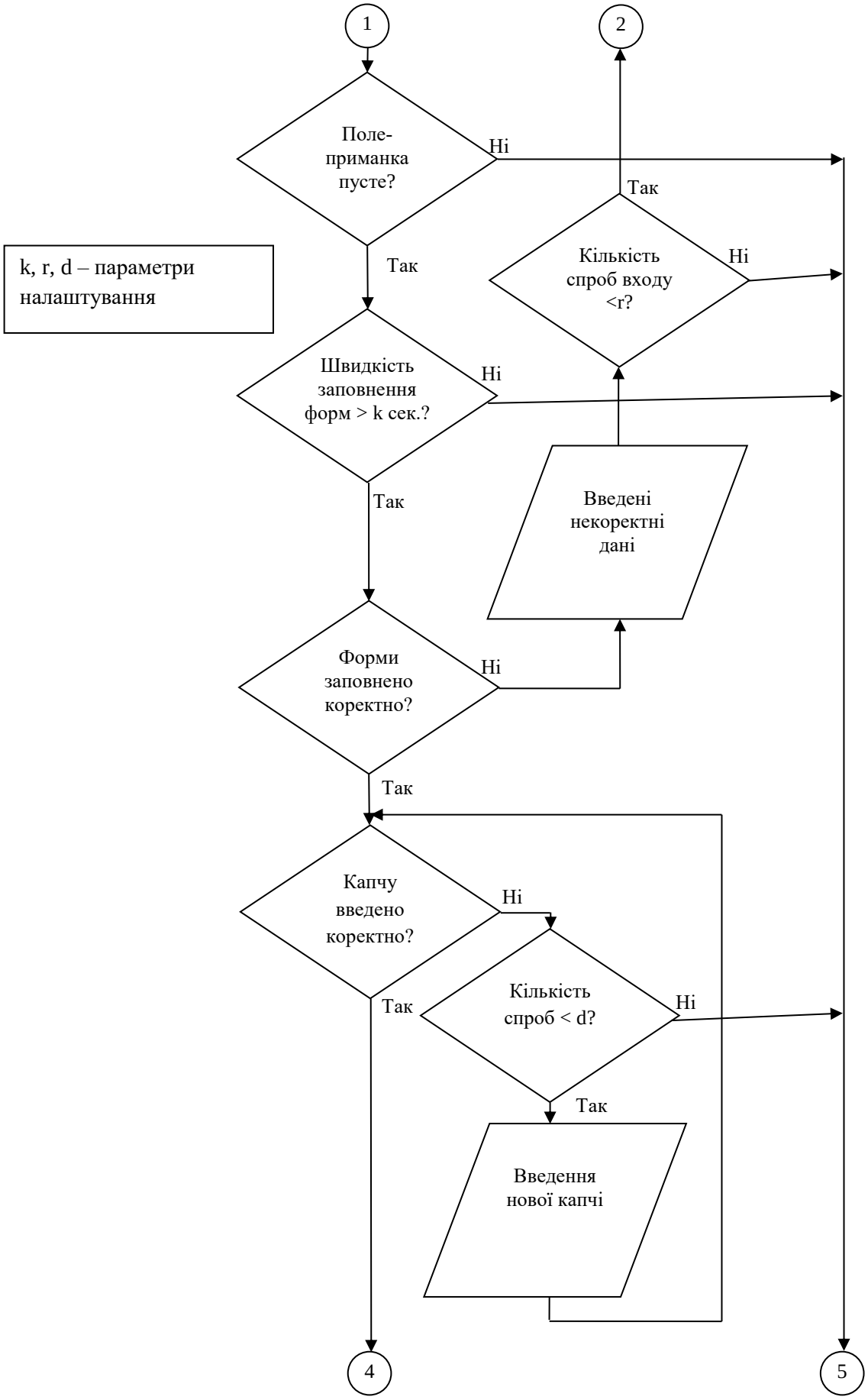
Послідовність, A_0 ... A_n, яка отримана після STOP – результат декодування.

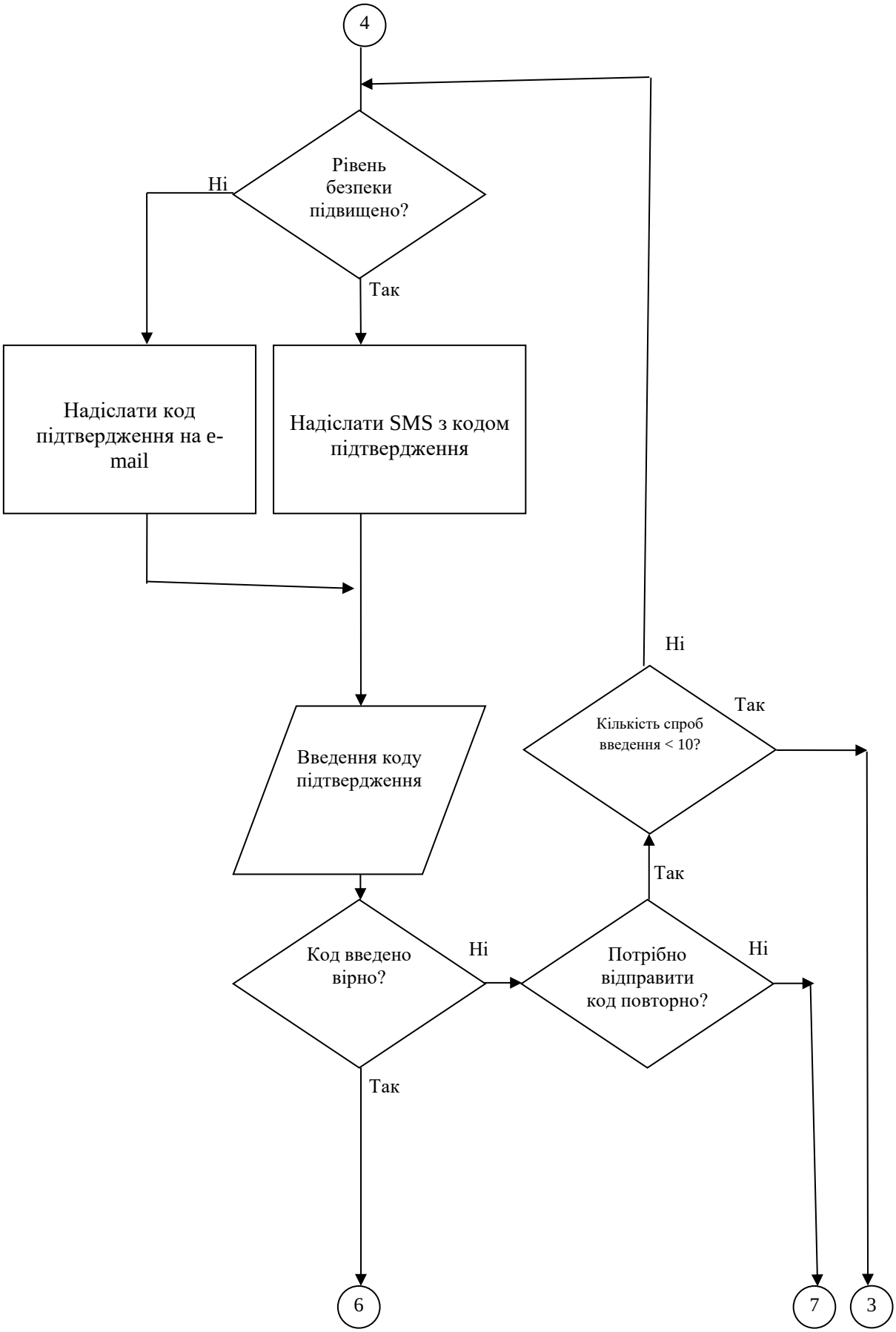
Якщо шифрування відбувається над текстовими даними, то вихідний файл (персональні дані) задля уникнення проблем із кодуванням символів в різних системах(Unicode, UTF8 тощо) буде містити зашифрований текст у форматі base64

Розроблений модульний алгоритм захисту від несанкціонованої реєстрації наведений на рисунку 3.1

.


Початок
Чи є даний IP в чорному списку?
Так
Ні
Чи є даний IP в публічному чорному списку?
Так
Підвищити рівень безпеки
Ні
Чи занесений IP в список для аналізу?
Так
t, n – значення налаштування
Ні
Чи отримано User-Agent?
Ні
Так
Внесення даних в поле реєстрації
1
2
3


1
2
Поле-приманка пусте?
Ні
Так
Так
Кількість спроб входу <r?
Ні
k, r, d – параметри налаштування
Швидкість заповнення форм > k сек.?
Ні
Так
Введені некоректні дані
Форми заповнено коректно?
Ні
Так
Капчу введено коректно?
Ні
Так
Кількість спроб < d?
Ні
Так
Введення нової капчі
4
5


4
Рівень безпеки підвищено?
Ні
Так
Надіслати код підтвердження на e-mail
Надіслати SMS з кодом підтвердження
Введення коду підтвердження
Код введено вірно?
Ні
Так
Потрібно відправити код повторно?
Ні
Так
Кількість спроб введення < 10?
Ні
Так
6
7
3

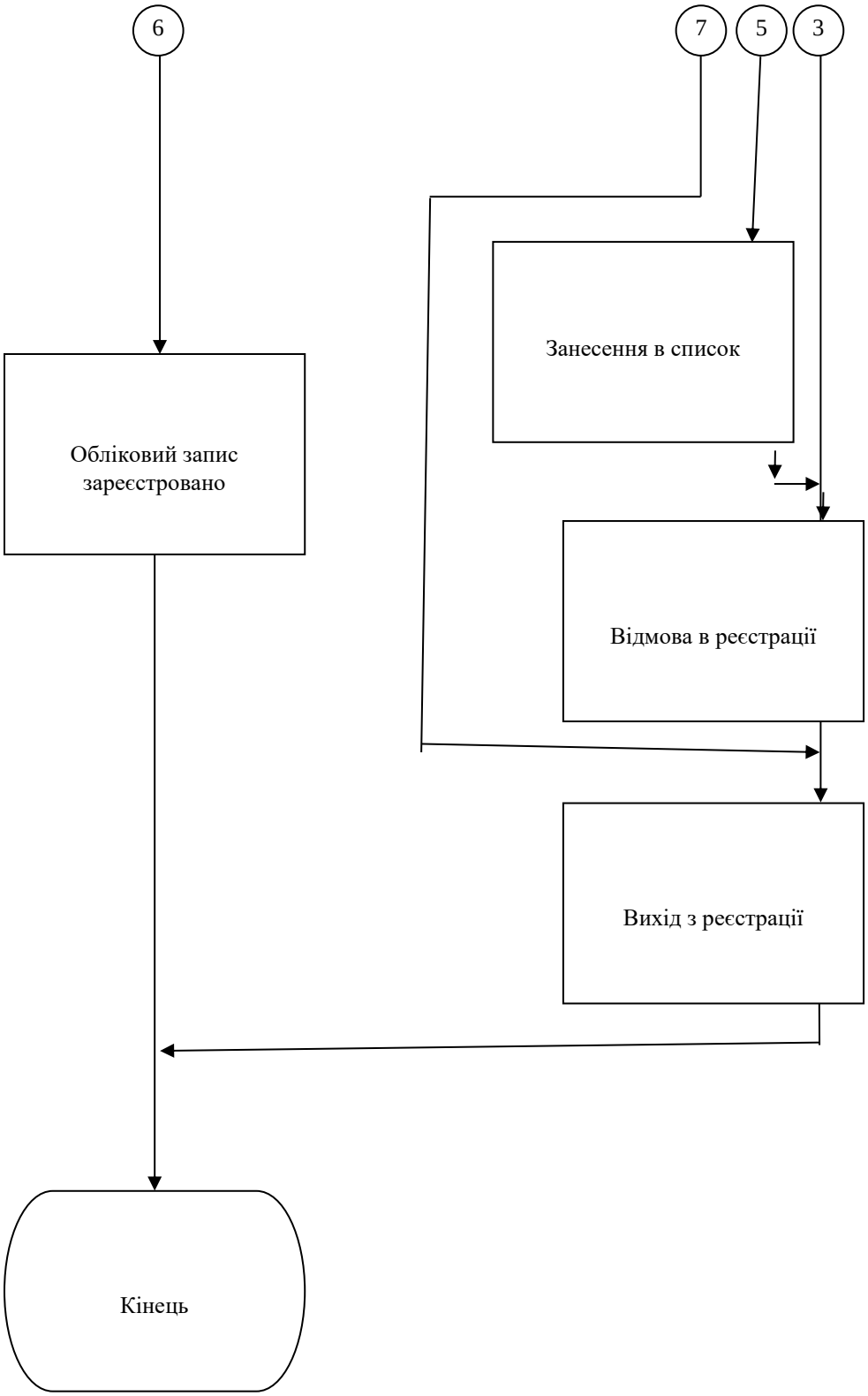


Рисунок 3.1 – Розроблений алгоритм захисту від несанкціонованої реєстрації

Висновки до розділу 3

В результаті написання третього розділу було вдосконалено існуючі аналоги політик безпеки соціальних мереж. Дана політика безпеки відрізняється від існуючих запровадженням модульного алгоритму захисту від несанкціонованої реєстрації, вдосконаленими алгоритмами захисту від несанкціонованого доступу, а також сучасним алгоритмом шифрування персональних даних соціальної мережі. Ці кроки дозволять підвищити захист персональних даних соціальної мережі.

ВИСНОВКИ

В результаті написання дипломної роботи виконано дослідження методів та умов реалізації політики конфіденційності й захисту персональних даних у соцмережах. Встановлено, що рішення захисту персональних даних у соціальних мережах формуються з урахуванням заходів організаційно-технічного характеру.

Оцінка ризиків порушення інформаційної безпеки показала актуальність захисту персональних даних в соціальних мережах.

Окрім того виділено основні методи захисту персональних даних в соціальних мережах від несанкціонованого доступу, серед яких найефективнішими є застосування різноманітних програмних засобів, таких як DLP, SIEM-системи, застосування криптографічних механізмів а також застосування двохфакторної автентифікації.

В роботі запропоновано вдосконалену політику захисту персональних даних соціальної мережі з використанням посиленого алгоритму захисту від несанкціонованої реєстрації та несанкціонованого доступу.

В результаті написання роботи були виконані наступні задачі:

1. Виконано огляд предметної області та показано актуальність захисту персональних даних в соціальних мережах.

2. Досліджено існуючі механізми та методи захисту персональних даних в соціальних мережах.

3. Розроблено рекомендації з підвищення захищеності даних в соціальних мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. — К.: Видавнича група ВНУ, 2016. — 608 с.

2. Закон України "Про інформацію" // ВВР. – 1992. – № 48. – Ст. 650. Вводиться в дію Постановою ВР від 02.10.92 №2658-12 // ВВР. – 1992. – №48. – Ст. 651.

3. Закон України "Про державну таємницю" // ВВР. – 1994. – № 16. – Ст. 93. Вводиться в дію Постановою ВР № 3856-XII від 21.01.94, ВВР, 1994, № 16, ст.94. Із змінами, внесеними згідно із Законами № 1169-VII від 27.03.2014.

4. Закон України "Про електронні документи та електронний документообіг" //ВВР. – 2003. – № 36. – Ст. 275. Із змінами, внесеними згідно із Законами № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст.349.

5. Закон України "Про електронний цифровий підпис" // ВВР. – 2003. – № 36. – Ст. 276. Із змінами, внесеними згідно із Законами № 879-VI від 15.01.2009, ВВР, 2009, № 24, ст.296 // № 5284-VI від 18.09.2012.

6. Закон "Про Національну програму інформатизації" // ВВР. – 1998. - № 27-28. - ст.181. Із змінами, внесеними згідно із Законами № 2684-III від 13.09.2001, ВВР, 2002, № 1, ст.3.

7. Закон "Про захист персональних даних" // ВВР. – 2010. - № 34. - ст. 481. Із змінами, внесеними згідно із Законами № 4452-VI від 23.02.2012, ВВР, 2012, № 50, ст.564.

8. Закон "Про захист інформації в інформаційно-телекомунікаційних системах" // ВВР. – 1994. - №31 - ст.286. Із змінами, внесеними згідно із Законами N 879-VI (879-17) від 15.01.2009, ВВР, 2009, № 24, ст.296.

9. Указ президента України " Про Положення про порядок здійснення криптографічного захисту інформації в Україні" // 22.05.1998, Л. Кучма № 505/98. Із змінами, внесеними згідно з Указами Президента // № 1019/98 (1019/98) від

15.09.98 // № 1229/99 (1229/99) від 27.09.99 // № 333/2008 (333/2008) від 11.04.2008 // № 693/2009 (693/2009) від 28.08.2009.

10. Конституція України. [Електронний ресурс] / Офіційний веб-сайт Верховної Ради України. - Режим доступу: http://portal.rada.gov.ua/.

11. Максимов Н.В. Технічні засоби інформатизації/Н.В. Максимов, М.: Форум, 2013 – 608 с.

12. Ярочкін В.І. Інформаційна безпека: підручник для студентів вищих навчальних закладів. - М.: Академічний проект; Гаудеамус, 2020. – 208 с.

13. Деркаченко А. Я. Соціальні мережі, як середовище для технологій маніпулятивного впливу [Електронний ресурс] / А. Я. Деркаченко. – 2016. – 25 с.

14. Радкевич О.П. Конфіденційність персональної інформації в соціальних мережах // Вісник Вищої ради юстиції. – 2012. – № 3(11). – С. 215-224.

15. Захист у соціальних мережах [Електронний ресурс]: Режим доступу: https://nris.ru/blog/zashita-v-socialnyh-setyah/ (дата звернення: 05.04.2022).

16. Хювенен, Е. Методи та системи програмування / Е. Хювенен, І. Септянен. – М.: [Гостехиздат], 2021. - 752 с.

17. Jorge Blasco, Julio Cesar Hernandez-Castro, Juan E Tapiador, and Arturo Ribagorda. Bypassing information leakage protection with trusted applications. computers & security, 31(4):557–568, 2012. – 256 p.

18. Rich Mogull and LLC Securosis. Understanding and selecting a data loss prevention solution. Technicalreport, SANS Institute, 2010. – 35 p.

19. Walter Rogowski. The right approach to data loss prevention. Computer Fraud and Security, 2013(8):5, 2013. – 42 p.

20. H. Balinsky, D. S. Perez, and S. J. Simske. System call interception framework for data leak prevention. pages 139–148. IEEE, 2011.

21. K. Kavanagh, T. Bussa, G. Sadowski. «Magic Quadrant for Security Information and Event Management». Gartner, 3 December 2018

22. Mozhaev O. Multiservise network security metric / O. Mozhaev, H. Kuchuk, N. Kuchuk, M. Mozhaev, M. Lohvynenco // IEEE Advanced information and

communication technologies-2017. Proc. of the 2th Int. Conf. – Lviv, 2017. – P. 133-136.

23. Франчук В.М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. Посібник для викладачів, вчителів та студентів інформатичних спеціальностей. – К.: НПУ імені М.П. Драгоманова, 2012. – 120 с.

24. Бабаш, А.В. Криптографічні методи захисту інформ.: Навчальний посібник: Т.1 / А.В. Бабаш. - М.: Риор, 2018. - 48 с.

25. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

26. Рябко, Б.Я. Криптографічні методи захисту інформації/Б.Я. Рябко, А.Н. Фионов. - М.: ГЛТ, 2013. - 229 с.

27. Остапов С. Е. О-76 Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

28. Сухов М.І., Гнєдіна О.А. Методи захисту у соціальних мережах. Молодий дослідник Дону, №2 (5) 2017. – с.32-35.

29. Домарьов В. В. Безпека інформаційних технологій. Системний підхід. Київ : ТОВ ТІД Діа Софт, 2004. - 992 с.

30. Поляк-Брагінський О.В. Локальна мережа. Найнеобхідніше, 2011. - 576 с.

31. Кавун С. В. Інформаційна безпека : навчальний посібник. Харків : ХНЕУ, 2008. - 352 с.

32. Сердюк В.О. Організація та технології захисту інформації. Виявлення та запобігання інформаційним атакам в автоматизованих системах підприємств: ВШЕ, 2013. - 576 с.