

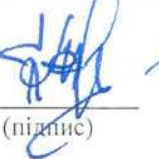
МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: Актуальні методи захисту інформації в умовах інформаційної війни

Здобувача вищої освіти другого (магістерського) рівня,
II курсу, групи КМІ-23-1, спеціальності 122 «Комп'ютерні науки»,
освітня програма «Інформаційні управляючі системи і технології в економіці»

	 (підпис)	<u>Данилка Ігоря Костянтиновича</u> (прізвище, ім'я, по батькові, науковий ступінь)
Науковий керівник	 (підпис)	<u>Філоненко М. М., к.ф.-м.н., доцент.</u> (прізвище, ім'я, по батькові, науковий ступінь)
Керівник освітньо- професійної програми	 (підпис)	<u>Горбовий А. Ю., д.т.н., професор</u> (прізвище, ім'я, по батькові, науковий ступінь)
Допущено до захисту за рішенням кафедри протокол від «10» січня 2025р № 11		
Завідувач кафедри	 (підпис)	<u>Філоненко М. М., к.ф.-м.н., доцент</u> (прізвище, ім'я, по батькові, науковий ступінь)

Ірпінь – 2025

Реєстрація № 22

27.01.2025

(дата)



(підпис відповідальної особи)

Результати перевірки

до захисту

(до захисту, на доопрацювання)

27.01.2025

(дата)



(підпис)

Результат захисту

4 (добре)

(оцінка)

06.02.2025

(дата)



(підпис)

Голова комісії:



(підпис)

В.М. Франчук

(ініціали, прізвище)

Члени комісії:



(підпис)

А.Ю. Горбовий

(ініціали, прізвище)



(підпис)

М.М. Філоненко

(ініціали, прізвище)



(підпис)

І.Д. Погореловська

(ініціали, прізвище)

БЛАНК ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст кваліфікаційної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	25		06.02.2025 Франчук В.М. 
2. Дотримання вимог щодо оформлення	від 0 до 10	8		Горбовий А.Ю. 
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	4		Філоненко М.М. 
4. Рецензент	від 0 до 5	4		Погореловська І.Д. 
РАЗОМ БАЛІВ	від 0 до 50	41		Суховерхівка Л.П. 

Оцінювання кваліфікаційної роботи науковим керівником - 39 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підпис)
80	B	4 (добре)	06.02.2025	Франчук В.М. 
				Горбовий А.Ю. 
				Філоненко М.М. 
				Погореловська І.Д. 
				Суховерхівка Л.П. 

ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	
50-59	E	3 (задовільно)
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій

Кафедра комп'ютерних та інформаційних технологій і систем

Галузь знань: 12 «Інформаційні технології»

Спеціальність: 122 «Комп'ютерні науки»

Освітня програма: «Інформаційні управляючі системи та технології в економіці»

Затверджую

Завідувач кафедри

Філоненко М. М

«23» грудня 2025р.

**Завдання на кваліфікаційну роботу
здобувачу вищої освіти**

Данилку Ігорю Костянтиновичу

1. Тема кваліфікаційної роботи: «Актуальні методи захисту інформації в умовах інформаційної війни»

Затверджена наказом ректора від «20» грудня 2023 р. № 1701

2. Строк здачі закінченої роботи: «07» січня 2025р.

Мета роботи: Огляд актуальних методів захисту інформації в умовах інформаційної війни

Об'єкт дослідження: __основи функціонування методів криптографічного перетворення.

Предмет дослідження: сучасні процедури захисту інформації.

3. Вихідні дані до роботи: загальні відомості про інформаційну війну, загрози та вразливості інформаційного простору, методи захисту інформації, державні та міжнародні ініціативи у сфері інформаційної безпеки

4. Перелік графічного матеріалу: Інфографіка про основні загрози інформаційної війни, схема, діаграма, діаграми, динамічні блок-схеми

5. Зміст кваліфікаційної роботи (перелік питань за кожним розділом):

Розділ 1: ОСНОВНІ ПОЛОЖЕННЯ ПРО ЗАХИСТ ІНФОРМАЦІЇ

1.1. Стратегія кібербезпеки України

1.2. Вимоги до захисту інформації web – сторінки від несанкціонованого доступу

1.3. Висновки по розділу

Розділ 2: АНАЛІЗ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Проблема захисту інформації

2.2. Методи і способи захисту інформації

2.3. Висновки по розділу

Розділ 3: ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ

3.1. Створення середовища для виконання дипломної роботи

3.2. Visual Studio - інтегроване середовище розробки ПЗ

3.3. Висновки по розділу

6. Календарний план виконання роботи

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Вибір теми, підбір літературних джерел, формування структури ДР	До 16.11.2023 р.	16.11.2023 р.
2	I розділ (розкрити сутність і стан дослідження наукової проблематики роботи, після чого навести її загальну характеристику; огляд літератури за темою і вибір конкретних напрямів досліджень)	26.03. 2024 р.	26.03. 2024 р.
3	II розділ (аналіз експериментальної частини про і методики досліджень)	20. 06.2024 р.	20. 06.2024 р.
4	III розділ (проведені теоретичні і (або) експериментальні дослідження та проектні рішення)	15.10.2024 р.	15.10.2024 р.
5	Висновки	20.11.2024 р.	20.11.2024 р.
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	20.01.2025 р.	20.01.2025 р.
7	Отримання відгуку керівника	25.01.2025 р.	25.01.2025 р.
8	Отримання зовнішньої рецензії	27.01.2025р.	До 16.11.2023 р.

Дата видачі завдання «23» грудня 2023 р.

Керівник дипломної роботи


(підпис)

Філоненко М. М.

Керівник освітньо-професійної програми


(підпис)

Горбовий А. Ю

Завдання до виконання отримав здобувач вищої освіти


(підпис)

Данилко І.К.

АНОТАЦІЯ

Анотація до дипломної роботи "Актуальні методи захисту інформації в умовах інформаційної війни"

Мета роботи- аналіз і захист даних в умовах інформаційної війни.

У роботі розглянуто основні загрози інформаційної безпеки, які виникають у контексті сучасних конфліктів, зокрема у сфері кібербезпеки, а також можливості протидії цим загрозам за допомогою інноваційних технологій та методик. Особлива увага приділяється аналізу засобів криптографії, систем аутентифікації та шифрування.

Також розглядається роль державних та приватних організацій у створенні комплексних стратегій кіберзахисту, а також правові та етичні аспекти, що виникають в умовах інформаційної війни. На основі проведеного дослідження розроблено рекомендації щодо вдосконалення заходів захисту інформації та підвищення стійкості інформаційних систем до атак в умовах гібридних загроз.

Ключові слова: інформаційна безпека, інформаційна війна, кіберзахист, криптографія, стеганографія, штучний інтелект, машинне навчання, кіберзагрози.

Рік виконання кваліфікаційної роботи: 2025.

Рік захисту роботи: 2025.

ABSTRACT

The purpose of the work is to analyze and protect data in the conditions of information warfare.

The work considers the main threats to information security that arise in the context of modern conflicts, in particular in the field of cyber security, as well as the possibilities of countering these threats with the help of innovative technologies and methods. Special attention is paid to the analysis of cryptography, authentication and encryption systems.

The role of government and private organizations in developing comprehensive cybersecurity strategies, as well as the legal and ethical aspects arising in the context of information warfare, is also examined. Based on the conducted research, recommendations have been developed for improving information protection measures and enhancing the resilience of information systems to attacks in the context of hybrid threats.

Keywords: information security, information warfare, cybersecurity, cryptography, steganography, artificial intelligence, machine learning, cyber threats.

Year of completion: 2025.

Year of defense: 2025.

ЗМІСТ

ВСТУП.....	4
Розділ 1: ОСНОВНІ ПОЛОЖЕННЯ ПРО ЗАХИСТ ІНФОРМАЦІЇ.....	6
1.1. Стратегія кібербезпеки України.....	6
1.2. Вимоги до захисту інформації web – сторінки від несанкціонованого доступу.....	9
1.3. Висновки по розділу.....	13
Розділ 2: АНАЛІЗ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ.....	24
2.1. Проблема захисту інформації.....	24
2.2. Методи і способи захисту інформації.....	32
2.3. Висновки по розділу.....	36
Розділ 3: ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ.....	37
3.1. Створення середовища для виконання дипломної роботи.....	37
3.2. Visual Studio - інтегроване середовище розробки ПЗ.....	39
3.3. Висновки по розділу	52
СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ.....	53

ВСТУП

Актуальність дослідження. Розвиток інформаційних комп'ютерних технологій надав можливість не тільки обмінюватися інформацією, а і змогу ведення бізнесу, збереженню інформації у мережі, тобто розширив можливості нашого кібер-простору. Зараз по всьому світу працює тисячі сайтів, які ведуть розрахунки онлайн. А безпечне зберігання та передавання цих розрахунків гарантувати ніхто не може. Розвиток інформаційних технологій дозволяє в значній мірі скоротити дистанцію між виробником і споживачем банківських послуг.

Ось на приклад: зі зростанням як внутрішнього, так і зовнішнього ринку зростає кількість програмістів, дизайнерів та подібних спеціалістів в області інформаційних послуг. Зазвичай акі професії вимагають навіть для навчання сучасні та швидкі комп'ютери але не всі мають можливість придбати професійні машини, які необхідні для їх діяльності. Попит породжує пропозиції, тому зараз існують заклади, вони ж офіси, в яких в аренду здаються робочі місця разом із професійними та не дешевими комплектуючими, які підходять для будь-яких, навіть, графічних робіт за дуже вигідними цінами. Але що робити, якщо необхідно працювати із інформацією, яка не підлягає розголошенню, а можливості придбати свій комп'ютер нема. Нікто не дасть гарантію, ніхто не стане працювати з вашим комп'ютером у час вашої відсутності.

Навіть державні підприємства та служби стикаються з тими самими загрозами. Справді, більшість застосунків зараз переміщується в хмару, але, незважаючи на передові методи автентифікації та найбезпечніші системи передавання даних, вони не застраховані від організаційних проблем, які дозволяють зловмисникам отримати потрібну інформацію. Зрештою, всі звикли до комфорту, використовують автозаповнення паролів і форм, пишуть паролі на папірці - це не така вже й велика проблема, але людський фактор залишає злодіям безліч можливостей. Адже більшість людей звикли до думки, що

зловмисники перебувають десь далеко. Безпека даних у відкритій інформаційній мережі, якою є Інтернет, завжди відкрита для атак. Тому вкрай важливо забезпечити безпечне передавання та оброблення даних, як і у випадку з персональними комп'ютерами. Адже навіть якщо мережа захищена і всі додатки перенесені в хмарні технології, все одно важливо, щоб дані для вільного доступу до ресурсів не потрапили в чужі руки, навіть якщо злодій - інсайдер.

Метою і завданням є аналіз і захист даних в умовах інформаційної війни.

Для досягнення цієї мети буде вирішено такі завдання:

-Вивчення відомих методів криптографічних систем і перетворень.

-Розробка та вибір методів і підходів для розподілу прав доступу та запобігання витоку конфіденційної інформації, заснованих на наукових дослідженнях.

-Розробка алгоритмів і програмного забезпечення на основі обраних і розроблених методів.

Об'єкт дослідження - основи функціонування методів криптографічного перетворення.

Предметом дослідження є сучасні процедури захисту інформації. Актуальність дослідження полягає в забезпеченні безпечного зберігання для забезпечення конфіденційності конфіденційних даних. Оскільки кількість крадіжок персональних даних зростає з кожним днем, необхідно вживати заходів захисту. Хешування та шифрування - це криптографічні методи, які розв'язують проблему крадіжки або зміни цінної інформації.

Новизна отриманих результатів полягає в тому, що змінено стандартну форму зберігання паролів і розроблено систему аналізу даних, що виключає витік персональних даних. Надійність криптографічних алгоритмів залежить від часу опрацювання функції, тому можливість використання сучасних і ефективних методів захисту інформації на старих і повільних комп'ютерах є одним з основних параметрів. Такий підхід дає змогу кожному користувачеві самостійно визначати ступінь надійності системи.

РОЗДІЛ 1. ОСНОВНІ ПОЛОЖЕННЯ ПРО ЗАХИСТ ІНФОРМАЦІЇ

1.1. Стратегія кібербезпеки України

Пункт 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються у таких значеннях - перехоплення інформації в системі - дія, що унеможливлює доступ до інформації в системі;

- витік інформації - результат дії, внаслідок якої інформація в системі стає відомою або доступною фізичним та/або юридичним особам, які не мають права доступу до цієї інформації;

- власник інформації - фізична або юридична особа власник системи - фізична або юридична особа, якій належать права на інформацію;

- доступ до інформації в системі - можливість користувача опрацьовувати інформацію в системі;

- захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі несанкціонованих дій щодо інформації в системі;

- знищення інформації в системі;

- дії, що призводять до зникнення інформації в системі;

- інформаційні (автоматизовані) системи - організаційно-технічні системи, в яких за допомогою технічних і програмних засобів реалізується технологія обробки інформації;

- інформаційно-комунікаційні системи - сукупності інформаційних і комунікаційних комплексів, що функціонують як єдине ціле в системі технологічного процесу обробки інформації;

- «Комплексна система захисту інформації» - сукупність взаємопов'язаних організаційних та інженерно-технічних засобів, засобів і методів захисту інформації. - «Користувач інформації в системі» (далі - користувач) - фізична або юридична особа, яка в установленому

законодавством порядку отримала право доступу до інформації в системі;

- обробка інформації в системі - виконання однієї або декількох операцій. Операції, що виконуються в системі за допомогою технічних і програмних засобів, такі як збирання, введення, запис, накопичення, перетворення, зчитування, зберігання, знищення, збереження, приймання, одержання, передача; - порушення цілісності інформації в системі;

- несанкціоновані дії, які стосуються інформації в системі та спричиняють зміни її змісту. порядок доступу до інформації в системі;

- технічний захист інформації - вид захисту інформації, спрямований на забезпечення запобігання витоку, знищенню, блокуванню, порушенню цілісності та доступу до інформації за допомогою інженерно-технічних засобів та/або програмно-технічних комплексів.

Пункт 2. Суб'єкти відносин

Суб'єктами захисту інформації в системі є - власники інформації;

- власники системи;
- користувачі;
- центральні органи виконавчої влади та їхні територіальні органи, спеціально уповноважені з питань організації приватного зв'язку та захисту інформації.

Пункт 3. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їхні повноваження щодо цієї інформації визначаються власником інформації. Порядок доступу до національних інформаційних ресурсів або інформації з обмеженим доступом, перелік користувачів, а у випадках, коли захист цієї інформації вимагається законом, їх повноваження щодо цієї інформації визначаються законом. У випадках, передбачених законом, доступ до інформації в системі може надаватися без дозволу власника в порядку, встановленому законом.

Пункт 4. Відносини між власником інформації та власником системи

Якщо інше не передбачено законом, володілець системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, укладеному з володільцем інформації. Власник системи зобов'язаний надавати інформацію про захист інформації в системі на вимогу володільця інформації.

Пункт 5. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи за погодженням з власником інформації, якщо інше не передбачено законом. Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації та перевірятися на відповідність вимогам. Підтвердження відповідності здійснюється за результатами національної експертизи в порядку, встановленому законом. Для створення комплексної системи захисту національних інформаційних ресурсів або інформації з обмеженим доступом використовуються засоби захисту інформації, що мають атестат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації, вимоги до захисту якої визначені законом. Підтвердження адекватності цих заходів та їх державна експертиза здійснюється в порядку, встановленому законодавством.

Пункт 6. Відповідальність за забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи. «Власник системи, в якій обробляються національні інформаційні ресурси або інформація з обмеженим доступом та визначено вимогу щодо їх захисту», повинен відповідно до закону створити службу захисту інформації або призначити особу, відповідальну за забезпечення захисту та управління інформацією. Власник системи зобов'язаний інформувати центральний орган виконавчої влади з питань спеціального зв'язку та захисту інформації зі спеціальними повноваженнями або його субрегіональні органи про спроби та/або випадки неправомірного

використання системи щодо національних інформаційних ресурсів або інформації з обмеженим доступом.

Пункт 7. Вимоги щодо забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом встановлюються законом та Кабінетом Міністрів України. центральні органи виконавчої влади, спеціально уповноважені на організацію спеціального зв'язку та захисту інформації: - формують пропозиції щодо державної політики у сфері захисту інформації та в межах своєї компетенції забезпечують їх реалізацію; - визначають вимоги та порядок створення комплексної системи захисту національних інформаційних ресурсів або інформації з обмеженим доступом (вимоги щодо їх захисту встановлюються законом); - вживають заходів щодо виявлення загроз національним інформаційним ресурсам внаслідок несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та вносять рекомендації щодо запобігання таким загрозам. Державні органи в межах своєї компетенції за погодженням із центральним органом виконавчої влади, спеціально уповноваженою державною організацією спеціального зв'язку та захисту інформації, або суб'єктами владних повноважень визначають особливості захисту національних інформаційних ресурсів або інформації з обмеженим доступом (вимоги щодо їх захисту встановлюються законом).

1.2. Про основні засади забезпечення кібербезпеки України

Закон визначає важливі інтереси людини, громадянина, суспільства та держави у кіберпросторі; правові та організаційні основи забезпечення захисту національних інтересів України; основні цілі, напрями та принципи державної політики у сфері кібербезпеки; повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, встановлює основні засади координації діяльності, спрямованої на забезпечення кібербезпеки.

Пункт 1. Визначення термінів

У цьому розділі наведені терміни мають таке значення:

- Індикатори кіберзагроз - це технічні дані, що використовуються для виявлення та реагування на кіберзагрози;

- Кібератаки - цілеспрямовані (умисні) дії, що здійснюються в кіберпросторі за допомогою електронних комунікацій (у тому числі інформаційно-комунікаційних технологій, програмних, апаратних та інших технічних і технологічних засобів та обладнання) і спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності та доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в системах зв'язку, та/або порушення конфіденційності, цілісності та доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в телекомунікаційних та/або технічних системах, що забезпечує несанкціонований доступ до цих ресурсів;

- Кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

- Кіберзагрози - наявні та потенційні явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі та негативно впливають на національну кібербезпеку, кіберзахист та кіберзахищеність об'єктів;

- Кіберзлочинність (комп'ютерна злочинність) - суспільно небезпечні протиправні діяння у кіберпросторі та/або з його використанням, відповідальність за які передбачена Кодексом України про кримінальну відповідальність та/або криміналізована міжнародними договорами України;

- Кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в

результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

- Об'єкти критичної інфраструктури (далі - об'єкти критичної інфраструктури) - об'єкти незалежно від форми власності, діяльність яких безпосередньо пов'язана із забезпеченням технологічних процесів та/або послуг, що мають критичне значення для економіки і промисловості, функціонування соціальної сфери та громадської безпеки, збій або порушення в роботі яких може негативно вплинути на національну безпеку і оборону України, довкілля, завдати шкоди майну та/або будь-чому з переліченого вище і які можуть негативно вплинути на будь-яке з цих підприємств, установ чи організацій.

- Національна телекомунікаційна мережа - це створена відповідно до закону сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку та інших систем зв'язку, що використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, призначених для поширення (передавання, приймання, створення, оброблення, зберігання) та захисту інформації, забезпечення захищених електронних комунікацій та надання комплексу сучасних захищених інформаційних послуг.

- Національні електронні інформаційні ресурси (далі - національні інформаційні ресурси) - систематизовані електронні інформаційні ресурси (у тому числі публічна інформація, національні інформаційні ресурси та інша інформація), що містять інформацію незалежно від її виду, змісту, форми, часу і місця створення, призначені для задоволення життєво важливих суспільних потреб громадян, окремих осіб, суспільства і держави. Електронний інформаційний ресурс - будь-яка інформація, створена, записана, оброблена або збережена в цифровій формі або в іншому нематеріальному вигляді за допомогою електронних, магнітних, електромагнітних, оптичних, технічних,

програмних або інших засобів;

Пункт 2. Суб'єкти забезпечення кібербезпеки

- Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

- Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

- Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

- Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

- міністерства та інші центральні органи виконавчої влади;
- місцеві державні адміністрації;
- органи місцевого самоврядування;
- правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;
- “Збройні Сили України, інші військові формування, утворені відповідно до закону;
- Національний банк України;
- підприємства, установи та організації, віднесені до об'єктів

критичної інфраструктури;

- суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Суб'єкти, відповідальні за забезпечення кібербезпеки, у межах своєї компетенції:

— вживають заходи для запобігання використанню кіберпростору в воєнних, розвідувально-підливних, терористичних та інших протиправних і злочинних цілях;

— здійснюють виявлення та реагування на кіберінциденти і кібератаки, а також усунення їх наслідків;— забезпечують обмін інформацією щодо поточних та потенційних кіберзагроз;— розробляють і впроваджують превентивні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

— організовують проведення аудиту інформаційної безпеки, зокрема на підконтрольних об'єктах та об'єктах, що знаходяться в їхній сфері управління;

— реалізують інші заходи для розвитку та забезпечення безпеки кіберпростору.

1.3. Стратегія кібербезпеки України

Швидкий розвиток інформаційних технологій поступово змінює світ. Вільний та відкритий кіберпростір розширює свободу та можливості для людей, сприяє розвитку суспільства, створює глобальний інтерактивний ринок ідей, досліджень та інновацій. Це стимулює відповідальну та ефективну роботу органів влади, активне залучення громадян до управління державою та вирішення місцевих питань, забезпечує прозорість і публічність влади, а також сприяє боротьбі з корупцією. Однак разом із перевагами цифрового світу та розвитком інформаційних технологій виникають нові загрози для національної

та міжнародної безпеки. Окрім інцидентів природного (ненавмисного) характеру, зростає кількість і потужність кібератак, що мають на меті інтереси окремих держав, груп та осіб.

Все частіше виникають випадки незаконного збору, зберігання, використання, знищення та поширення персональних даних, а також незаконних фінансових операцій, крадіжок і шахрайства в Інтернеті. Кіберзлочинність стає глобальною проблемою, здатною завдати суттєвої шкоди інтересам осіб, суспільства та держави. Метою Стратегії кібербезпеки України (далі — Стратегія) є створення умов для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства та держави.

Загрози кібербезпеці

Кіберпростір поступово стає окремою сферою для ведення бойових дій поряд з традиційними сферами "Земля", "Повітря", "Море" та "Космос", де дедалі активніше діють відповідні підрозділи збройних сил провідних держав світу. З огляду на широке застосування сучасних інформаційних технологій у секторі безпеки та оборони, а також створення єдиної автоматизованої системи управління Збройних Сил України, оборона нашої держави стає більш вразливою до кіберзагроз. Економічна, науково-технічна, інформаційна сфери, а також державне управління, оборонно-промисловий комплекс, транспортна інфраструктура, сектор електронних комунікацій і безпеки України стають усе більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Сучасні інформаційно-комунікаційні технології можуть бути використані для вчинення терористичних актів, зокрема шляхом порушення нормальної роботи автоматизованих систем управління технологічними процесами на об'єктах критичної інфраструктури. Все більш поширеною стає політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні вебсайти в Інтернеті.

Національна система кібербезпеки, основні суб'єкти забезпечення кібербезпеки.

Національна система кібербезпеки повинна забезпечити взаємодію між державними органами, органами місцевого самоврядування, військовими формуваннями, правоохоронними органами, науковими установами, навчальними закладами, громадськими організаціями, а також підприємствами, установами та організаціями незалежно від форми власності, які займаються діяльністю в галузі електронних комунікацій, захисту інформації або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Основу національної системи кібербезпеки складатимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які згідно з порядком покладаються такі основні завдання:

— Міністерство оборони України та Генеральний штаб Збройних Сил України, відповідно до своєї компетенції, мають здійснювати заходи з підготовки країни до відбиття воєнної агресії в кіберпросторі (кібероборони), а також реалізовувати військову співпрацю з НАТО в межах безпеки кіберпростору та спільного захисту від кіберзагроз. Вони повинні забезпечити, у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України, кіберзахист власної інформаційної інфраструктури;

— Державна служба спеціального зв'язку та захисту інформації України має відповідати за формування та реалізацію державної політики з захисту державних інформаційних ресурсів та інформації, що підлягає захисту згідно із законом, кіберзахисту критичної інформаційної інфраструктури, а також за державний контроль у цих сферах. Вона повинна координувати діяльність інших суб'єктів кібербезпеки щодо кіберзахисту, а також здійснювати

організаційно-технічні заходи для запобігання, виявлення та реагування на кіберінциденти й кібератаки, усунення їх наслідків, інформування про кіберзагрози та методи захисту від них. Крім того, вона забезпечує функціонування державного центру кіберзахисту та проводить аудит захищеності об'єктів критичної інформаційної інфраструктури на вразливість.

— Служба безпеки України відповідає за попередження, виявлення, припинення та розслідування злочинів проти миру і безпеки людства, скоєних у кіберпросторі.

— Національна поліція України відповідає за захист прав і свобод людини, інтересів суспільства і держави від злочинних посягань у кіберпросторі, а також за запобігання, виявлення, припинення та розкриття кіберзлочинів, займається підвищенням поінформованості громадян щодо безпеки в кіберпросторі;

Пріоритети та напрями забезпечення кібербезпеки України

Розвиток безпечного, стабільного та надійного кіберпростору має включати, насамперед, такі аспекти:

- розробку та оперативну адаптацію державної політики в сфері кібербезпеки, орієнтуючись на розвиток кіберпростору і досягнення сумісності з європейськими та НАТО стандартами;
- створення національної нормативно-правової та термінологічної бази в цій сфері, гармонізацію нормативних актів у галузі електронних комунікацій, захисту інформації та кібербезпеки з міжнародними стандартами, а також стандартами ЄС та НАТО;
- формування конкурентного середовища у сфері електронних комунікацій та надання послуг із захисту інформації і кіберзахисту;
- розвиток технологій кіберзахисту для засобів мобільного зв'язку, забезпечення безпеки апаратних засобів, контенту, додатків та сервісів зв'язку;
- залучення наукових установ, професійних і громадських об'єднань до підготовки концептуальних документів у сфері кібербезпеки;
- підвищення цифрової грамотності громадян і розвитку культури

безпечного поведження в кіберпросторі, покращення знань, навичок і здібностей для підтримки цілей кібербезпеки, а також реалізація державних і громадських проектів для підвищення обізнаності суспільства щодо кіберзагроз і кіберзахисту;

- проведення навчань для реагування на надзвичайні ситуації та інциденти в кіберпросторі;

- удосконалення системи державного контролю за захистом інформації, а також системи незалежного аудиту інформаційної безпеки з упровадженням найкращих міжнародних практик і стандартів кібербезпеки.

Кіберзахист державних електронних інформаційних ресурсів та інфраструктури, призначеної для обробки інформації, захист якої передбачений законом, має бути орієнтований, передусім, на:

- створення та забезпечення функціонування національної телекомунікаційної мережі як єдиної платформи для захищених електронних комунікацій органів державної влади;

- впровадження організаційно-технічної моделі національної системи кібербезпеки та забезпечення оперативного реагування на кібератаки і кіберінциденти;

- розгортання (відповідно до компетенції) єдиної системи ситуаційних центрів відповідних органів державної влади в секторі безпеки та оборони на базі захищеної інформаційної інфраструктури;

- розбудова інтегрованої захищеної системи електронних державних реєстрів, баз даних, дата-центрів, включаючи єдиний дата-центр для резервного збереження інформації та даних державних електронних ресурсів;

- удосконалення системи зберігання, передачі та обробки даних державних реєстрів і баз даних із застосуванням сучасних інформаційно-комунікаційних технологій (зокрема онлайн-доступу);

- розробка нових методів запобігання кібератакам, кіберінцидентам та поширенню інформації про них;

— розробка вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами.

— підвищення рівня обізнаності працівників державних органів у питаннях інформаційної безпеки та кібербезпеки через проведення тренінгів і навчань;

Кіберзахист критичної інфраструктури має включати, зокрема:

— комплексне вдосконалення правової бази кіберзахисту об'єктів критичної інфраструктури, встановлення критеріїв для визначення інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем як частини критичної інформаційної інфраструктури;

— створення і підтримка функціонування державного реєстру об'єктів критичної інформаційної інфраструктури;

— визначення вимог до кіберзахисту для об'єктів критичної інфраструктури;

— організація та забезпечення функціонування підрозділів кіберзахисту на об'єктах критичної інфраструктури їх власниками або розпорядниками;

— встановлення кваліфікаційних вимог до працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій у галузі кібербезпеки та актуальних кіберзагроз, а також запровадження обов'язкової періодичної атестації таких працівників;

— налагодження співпраці між суб'єктами кіберзахисту критичної інфраструктури, розвиток державно-приватного партнерства для запобігання кіберзагрозам, реагування на кібератаки та кіберінциденти, а також для усунення їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного або воєнного стану, в особливий період.

Розвиток потенціалу сектору безпеки і оборони у сфері кібербезпеки включатиме вжиття таких заходів:

— забезпечення захисту технологічних процесів на об'єктах критичної

інфраструктури, що використовують інформаційно-комунікаційні технології для управління або моніторингу, від несанкціонованих вторгнень;

- регулярний огляд національної системи кібербезпеки та розробка галузевих індикаторів стану кібербезпеки;

- організація навчань для суб'єктів сектору безпеки і оборони з реагування на кібератаки та кіберінциденти, включаючи кібернавчання Збройних Сил України та інших органів, участь у навчаннях в рамках колективної оборони;

- реалізація стратегічного планування та програмно-цільового забезпечення розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту.

- проведення воєнно-політичних, військово-технічних та інших заходів для посилення можливостей Воєнної організації держави та сектору безпеки і оборони у кіберпросторі, створення та розвитку сил, засобів і інструментів для реагування на агресію в кіберпросторі, що може бути використано як засіб стримування військових конфліктів і кіберзагроз (активний кіберзахист);

- формування єдиного підрозділу для забезпечення кібербезпеки та кіберзахисту Збройних Сил України на стратегічному, оперативному та тактичному рівнях;

- розвиток та координація наукових досліджень у сфері кібербезпеки та кіберзахисту для потреб національної безпеки і оборони;

- підвищення здатності органів боротьби з кібертероризмом до протидії кібератакам на державні електронні інформаційні ресурси, об'єкти критичної інфраструктури, а також діяльності іноземних спецслужб, організацій, груп і осіб, які ведуть розвідувально-підбивну діяльність проти України в кіберпросторі.

- розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), комп'ютерних

систем і мереж, а також мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури та інших об'єктів, з відповідним розмежуванням підслідності;

Боротьба з кіберзлочинністю передбачатиме реалізацію таких заходів:

- створення ефективного контакт-центру для повідомлень про кіберзлочини та шахрайство в кіберпросторі, з підвищенням оперативності реагування на кіберзлочини правоохоронними органами, зокрема їх регіональними підрозділами.

- удосконалення процесуальних механізмів збору доказів у електронному форматі, що стосуються злочинів, а також покращення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, організація експертних досліджень;

- уніфікація порядку внесення обов'язкових до виконання приписів операторами та провайдерами телекомунікацій щодо термінового фіксування і подальшого зберігання комп'ютерних даних та даних про трафік;

- врегулювання можливості здійснення термінових процесуальних дій у реальному часі з використанням електронних документів та електронного цифрового підпису;

- впровадження протоколу координації правоохоронних органів для боротьби з кіберзлочинністю;

- підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з електронними доказами, що стосуються злочинів, враховуючи специфіку кіберзлочинів;

- запровадження спеціального порядку зняття інформації з каналів телекомунікацій під час розслідування кіберзлочинів;

- підвищення кваліфікації співробітників правоохоронних органів.

1.4. Вимоги до захисту інформації web – сторінки від несанкціонованого доступу

Цей нормативний документ системи технічного захисту інформації (НД

ТЗІ) визначає вимоги до технічних та організаційних заходів щодо захисту інформації на WEB-сторінках в Інтернеті. Згідно зі специфікаціями НД ТЗІ 2.5-004-99, документ встановлює мінімальний перелік послуг безпеки інформації та рівнів їх реалізації в комплексах засобів захисту WEB-сторінок від несанкціонованого доступу. Метою цього НД ТЗІ є надання нормативно-методологічної основи для розробки комплексу засобів захисту від несанкціонованого доступу до інформації на WEB-сторінках у рамках створення комплексної системи захисту інформації. Цей документ призначений для суб'єктів, діяльність яких пов'язана з розробкою та експлуатацією WEB-сторінок (власників, розпорядників, операторів, провайдерів, користувачів), розробників комплексних систем захисту інформації, постачальників окремих компонентів таких систем, а також для фізичних та юридичних осіб, які оцінюють захищеність WEB-сторінок на відповідність вимогам ТЗІ.

Вимоги, встановлені цим НД ТЗІ, є обов'язковими для виконання державними органами, Збройними Силами України, іншими військовими формуваннями, створеними відповідно до законів України, Радою Міністрів Автономної Республіки Крим та органами місцевого самоврядування, а також підприємствами, установами та організаціями (далі – установи) незалежно від форми власності при захисті інформації, що належить до державних інформаційних ресурсів на WEB-сторінках.

Визначення

У цьому НД ТЗІ використовуються терміни та визначення, що відповідають вимогам ДСТУ 2226 та НД ТЗІ 1.1-003. Інші терміни, вжиті в цьому НД ТЗІ, мають такі значення:

Інтернет (мережа Інтернет) – сукупність мереж і обчислювальних засобів, що використовують стек протоколів TCP/IP, спільний простір імен та адрес для забезпечення доступу до інформаційних ресурсів мережі для будь-якої особи;

Оператор (провайдер) – юридична або фізична особа, яка надає користувачам

доступ до мережі Інтернет;

Браузер – програмне забезпечення, що надає інтерфейс для доступу до інформації на WEB-сторінках та їх перегляду.

Робоча станція (клієнт мережі) – окремий (персональний) комп'ютер або віддалений термінал, з яких користувачі отримують доступ до ресурсів Інтернету.

Сервер – компонент комп'ютерної системи (програмний або програмно-апаратний пристрій), що надає послуги іншим системам за їх запитами.

WEB-сервер – сервер, який обробляє запити користувачів (клієнтів) за протоколом HTTP, відповідає за актуалізацію і збереження інформації на WEB-сторінці та взаємодіє з іншими серверами.

WEB-сторінка (WEB-сайт) – мережевий ресурс, який надається користувачу у вигляді HTML-документа і має унікальну адресу в Інтернеті.

HTML-документ – файл текстового або мультимедійного формату (звукові, відео або графічні файли), створений з використанням мови гіпертекстової розмітки HTML.

Посилання (гіпертекстове посилання) – адреса іншого мережевого ресурсу у форматі URL, що має тематичний, логічний чи інший зв'язок з документом, у

Характеристика типових умов функціонування та вимоги до захисту інформації WEB-сторінки

До складу АС, що забезпечує функціонування WEB-сторінки, входять: операційна система, фізичне середовище, в якому вона функціонує, середовище користувачів, оброблювана інформація, а також технологія її обробки. При забезпеченні захисту інформації необхідно враховувати всі характеристики цих складових, які можуть впливати на реалізацію політики безпеки WEB-сторінки. Якщо WEB-сторінка містить посилання на інформаційні ресурси інших WEB-сторінок, умови їх функціонування не повинні суперечити політиці безпеки, встановленій для цієї сторінки. У цьому розділі визначаються стандартні умови функціонування всіх складових АС, вводяться обмеження щодо їх роботи та

встановлюються загальні вимоги до захисту інформації для окремих компонентів АС. Для такої типово визначеної схеми функціонування АС пропонуються варіанти вибору функціональних профілів захисту інформації від несанкціонованого доступу (НСД).

1.5. Висновки по розділу

На сьогоднішній день зберігання даних неможливе без використання як криптографічних методів, так і механізмів розмежування прав доступу. Процедури ідентифікації та автентифікації активно застосовують сучасні криптографічні технології, а більшість сервісів і служб використовуються віддалено через Інтернет. Забезпечення належного контролю за цілісністю та доступністю інформації є основними критеріями, які повинні виконуватися в сучасних системах. Для розмежування прав доступу застосовуються різні методи автентифікації, від біометричних до парольних, проте це не має сенсу, якщо інформація зберігається в незахищеному вигляді.

РОЗДІЛ 2. АНАЛІЗ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Проблема захисту інформації

Інформаційні ресурси, як держави, так і суспільства загалом, а також окремих організацій і фізичних осіб, є цінними, мають матеріальну основу і потребують захисту, оскільки несанкціонований доступ може призвести до збитків і зменшення їхньої вартості. Впливи, які можуть призвести до зниження цінності інформаційних ресурсів, називаються негативними. Потенційно можливі негативні впливи вважаються загрозами. Захист оброблюваної інформації полягає в розробці та підтримці ефективної системи заходів, що включає технічні, інженерні, програмно-апаратні, а також правові та організаційні методи, які дозволяють запобігти або ускладнити реалізацію загроз і зменшити потенційні збитки. Такий захист є необхідним як у мирний час, так і під час інформаційної війни. Приватні та державні підприємства та організації мають конфіденційну та персональну інформацію, яку потрібно захищати від витоків і збитків. Іншими словами, захист інформації спрямований на забезпечення безпеки оброблюваних даних у цілому, тобто на підтримку таких властивостей інформації, що її обробляє. Система заходів, що забезпечує цей захист, називається комплексною системою захисту інформації.

На даний момент при вирішенні технічних проблем захисту інформації значну загрозу конфіденційності створюють організаційні та комунікаційні проблеми. Наприклад, з ростом як внутрішнього, так і зовнішнього ринку в країні збільшується кількість програмістів, дизайнерів, архітекторів та інших фахівців у галузі інформаційних послуг. Ці професії часто вимагають сучасних і потужних комп'ютерів, але не всі мають можливість придбати відповідне обладнання. Попит на такі ресурси сприяє появі офісів, де можна орендувати робочі місця з професійними комп'ютерами, що підходять навіть для графічних робіт, за доступними цінами. Це дозволяє навіть студентам користуватися

подібними послугами. Однак виникає питання: як працювати з конфіденційною інформацією, коли немає можливості придбати власний комп'ютер? У таких випадках неможливо отримати гарантії безпеки, і навіть якщо комп'ютер залишатиметься на місці, коли вас немає, ризик зловживання залишається високим, оскільки велика кількість людей, з якими ви не знайомі, має доступ до цього обладнання.

Ці самі проблеми стосуються й державних підприємств та служб. Хоча багато програм зараз працюють на хмарних технологіях, навіть вони не застраховані від організаційних проблем, через які зловмисники можуть отримати доступ до конфіденційної інформації, попри використання передових методів аутентифікації та найсучасніших систем передачі даних. Люди звикли до зручності: вони використовують автозаповнення паролів, зберігають їх на папірцях або на незахищених носіях. Хоча це не є безпечним, людський фактор часто залишає багато можливостей для зловмисників, оскільки більшість людей вважає, що небезпека завжди далеко, і тому не надають достатньої уваги безпеці своїх даних.

Зі збільшенням вартості та серйозності кібератак уряд спробував розробити ефективні рішення. Державні та місцеві політики здійснили низку заходів, щоб залучити державні та приватні підприємства до посилення кібербезпеки, включаючи дії в рамках виконавчої та законодавчої влади. Однак ці заходи, часто спричинені необхідністю реагувати на резонансні кіберінциденти, часто є неефективними та фрагментарними. Хоча спрямовані нормативні акти пропонують загальний, але чіткий підхід уряду до зменшення кіберризиків, виконавчі агенції не відповідають належним чином на зміцнення державних активів, операцій та інструментів для захисту від атак.

Ті, хто працює в оборонній промисловості, змушені долати складний і багатошаровий набір політичних регламентів, що включають окремі органи влади та суперечливі інституційні агенти. Це неприязне регуляторне середовище створює бар'єри навіть для найбільших оборонних підрядників і є

головною перепорою для впровадження кращих практик кібербезпеки. Представлені резюме регуляторних органів, які безпосередньо відповідають за таке середовище, сприяють розмежуванню та роз'ясненню нової хвилі кіберрегламентів.

Будь-яка оцінка ефективності політики реагування на кіберзагрози є неповною без урахування перспектив оборонної промисловості. Як перша лінія оборони та об'єкт нових і чинних норм, її учасники мають унікальну кваліфікацію для оцінки поточної ситуації. Для цього був розроблений інструмент обстеження, щоб зібрати думки галузі. Включено запитання щодо оцінки фінансових наслідків дотримання кіберполітики, визначення найкращих практик кіберзахисту та аналіз ставлення галузі до чинних кіберзаконів.

Посилення комунікацій, оптимізація потоку інформації та спрощення поточного режиму кіберрегулювання є першочерговими кроками, які уряд має зробити для підвищення операційної безпеки оборонної промисловості. Існує розрив між великими, стабільними підприємствами та малими компаніями в аспектах кіберінформованості, готовності та відповідності вимогам. Малому бізнесу необхідні спеціалізовані урядові комунікації та ресурси для того, щоб вони залишалися частиною промислового ланцюга постачання. Нова політика повинна також об'єднати регуляторні органи для зменшення навантаження на відповідність, враховуючи поточний досвід і досвід галузевих партнерів під час розробки та впровадження політики.

Ризик розкриття інформації вже давно є предметом занепокоєння в статистичних та інформаційних спільнотах, і для його обмеження було розроблено кілька методів. Контроль за статистичним розкриттям даних спрямований на те, щоб дозволити робити корисні висновки про субпопуляції на основі даних, одночасно забезпечуючи конфіденційність осіб, що надали ці дані. Для зниження ризику розкриття інформації при публікації мікроданих було запропоновано кілька підходів SDC. Їх спільною рисою є те, що оригінальний набір даних залишається конфіденційним, а публікується лише

модифікована анонімізована версія. Останнім часом було запропоновано кілька моделей конфіденційності, які не фокусуються на конкретних трансформаціях початкових даних, а визначають умови, яким має відповідати набір даних, щоб мінімізувати ризик розкриття.

Одним з основних недоліків великих даних є потенційний ризик для конфіденційності. Важливо розуміти, що великі дані передбачають збір максимальної кількості інформації для отримання знань. Більше того, ці дані часто надаються не безпосередньо суб'єктом інформації, таким як споживач чи громадянин, а виникають як побічний продукт транзакцій, наприклад, перегляду чи покупки товарів в інтернет-магазинах. Також ці дані можуть збиратися постачальниками послуг у вигляді компенсації за безкоштовні сервіси, наприклад, облікові записи електронної пошти чи соціальні мережі, або як частина вимог до певних послуг, наприклад, GPS-навігаційна система потребує інформації про місце розташування користувача, щоб надати актуальну інформацію про дорожні умови.

На сьогоднішній день не існує універсальної стратегії захисту конфіденційності для великих даних. До появи великих даних принципи захисту особистої інформації застосовувалися в різних регламентах, що стосуються ідентифікації та захисту даних:

- **Законність.** Згода повинна бути отримана від суб'єкта, або обробка даних має бути необхідною для виконання договору чи юридичних зобов'язань, життєвих інтересів суб'єкта, суспільних інтересів або законних інтересів обробника, що узгоджуються з правами суб'єкта.

- **Згода.** Згода суб'єкта повинна бути чіткою, конкретною, інформованою та явною.

- **Обмеження мети.** Мета збору даних повинна бути законною та визначеною до їх збору.

- **Необхідність і мінімізація даних.** Збирати слід лише ті дані, які необхідні для досягнення конкретних цілей, і зберігати їх лише стільки, скільки

потрібно.

— **Права суб'єктів даних.** Суб'єкти повинні мати доступ до своїх даних, а також можливість виправити або видалити їх (право бути забутим).

— **Інформаційна безпека.** Зібрані дані повинні бути захищені від несанкціонованого доступу, обробки, маніпулювання, втрати або знищення.

— **Прозорість і відкритість.** Суб'єкти повинні отримувати інформацію про збір та обробку їхніх даних у спосіб, який вони можуть зрозуміти.

— **Підзвітність.** Особи, що здійснюють збір та обробку даних, повинні мати змогу демонструвати відповідність вищезазначеним принципам.

— **Захист даних за замовчуванням та на етапі проектування.** Конфіденційність повинна бути вбудована в систему з самого початку, а не додаватися пізніше.

Без анонімізації виникають кілька потенційних конфліктів між зазначеними принципами та метою великих даних:

— **Обмеження мети.** Великі дані часто використовуються повторно для цілей, які не були передбачені на момент збору.

— **Згода.** Якщо мета збору даних не зрозуміла, отримати згоду неможливо.

— **Законність.** Без обмеження мети та згоди правомірність використання даних може бути поставлена під сумнів.

— **Необхідність і мінімізація даних.** Великі дані є результатом збору інформації для потенційного використання в майбутньому.

— **Індивідуальні права.** Окремі суб'єкти навіть не знають, які дані про них зберігаються, і хто їх зберігає, що ускладнює доступ до даних, їх виправлення або видалення.

— **Підзвітність.** Відсутність відповідності означає неможливість продемонструвати дотримання принципів конфіденційності.

Враховуючи ці конфлікти між принципами конфіденційності та великими даними, деякі стверджують, що для того, щоб уникнути перешкод для

технологічного розвитку, захист конфіденційності має зосереджуватися лише на використанні даних, які можуть завдати шкоди конфіденційності, а не на зборі даних або навіть дозволяти саморегуляцію. Водночас інша точка зору полягає в тому, що саме збір даних є основною причиною потенційних порушень конфіденційності. Дійсно, після збору даних виникає багато можливих загроз.

— **Порушення безпеки даних.** Це може статися через агресивні злому чи недостатні заходи безпеки. Чим більше даних зібрано, тим привабливішими вони стають для зловмисників.

— **Внутрішнє зловживання співробітниками.**

— **Невиконання умов щодо вторинного використання даних.**

— **Зміни в політиці компанії.** Політика, що обмежує участь компанії у використанні даних, які можуть завдати шкоди інтересам суб'єктів, може бути змінена.

— **Методи анонімізації** — це можливе рішення для зменшення конфліктів між принципами конфіденційності та великими даними.

Проте методи анонімізації мають певні труднощі при застосуванні до великих даних. З одного боку, недостатня анонімізація, наприклад, просте видалення прямих ідентифікаторів, може не забезпечити достатнього рівня неідентифікованості. Це стає більш проблематичним для великих даних, оскільки велика кількість і різноманітність інформації про особу збільшує ймовірність повторної ідентифікації. З іншого боку, надмірна анонімізація може ускладнити зв'язування даних про одну і ту ж особу або групи осіб із різних джерел, що може обмежити багато потенційних переваг великих даних.

Технології, такі як глобальне перекодування, придушення, кодування верхнього та нижнього, мікроагрегація, застосовують перетворення даних, спрямовані на зменшення ризику розкриття інформації. Однак, загалом, вони не включають чітких механізмів для оцінки залишкового ризику розкриття в оброблених даних. Реальність полягає в тому, що більшість моделей

конфіденційності були розроблені для захисту статичних, оригінальних наборів даних, що накладає серйозні обмеження на їх застосування до великих обсягів даних.

Три основні характеристики, які часто асоціюють з великими даними, — це об'єм, різноманітність і швидкість. Об'єм стосується великої кількості даних, що підлягають аналізу. Різноманітність означає, що великі дані складаються з різних типів даних, які отримані та об'єднані з різних джерел. Швидкість вказує на темп генерації та обробки даних. Не всі ці характеристики повинні обов'язково бути присутніми для того, щоб дані можна було вважати великими, але хоча б деякі з них є необхідними.

Щоб модель конфіденційності була ефективною в умовах великих даних, вона повинна добре працювати з об'ємом, різноманітністю та швидкістю. Для оцінки її придатності для великих даних необхідно перевірити, наскільки вона відповідає трьом ключовим вимогам:

1. **Композиційність.** Модель конфіденційності є композиційною, якщо гарантії конфіденційності зберігаються, хоча б частково, після багаторазового незалежного застосування цієї моделі. Якщо ж кілька окремих випусків даних, кожен із яких відповідає вимогам моделі, можуть призвести до порушення конфіденційності, то модель не є композиційною.

2. **Скалярність.** Модель конфіденційності має бути масштабованою, тобто вона повинна ефективно працювати з великими обсягами даних. Це означає, що навіть за значного збільшення обсягу даних модель повинна залишатися стабільною та забезпечувати відповідний рівень захисту конфіденційності без істотних втрат у продуктивності або точності.

3. **Адаптивність.** Модель повинна бути здатна адаптуватися до змін у даних та середовищі, в якому вони обробляються. Оскільки великі дані постійно оновлюються та змінюються, модель конфіденційності повинна бути гнучкою і дозволяти коригувати свої параметри в залежності від нових даних або змін у політиках безпеки.

Обчислювальна вартість. Обчислювальна вартість визначає кількість ресурсів, необхідних для перетворення вихідного набору даних у такий, що відповідає вимогам моделі конфіденційності. Як вже згадувалося, існує широкий вибір методів SDC, які можна застосувати для забезпечення відповідності моделі конфіденційності. Тому обчислювальна вартість залежить від обраного методу SDC. Оцінюючи вартість моделі конфіденційності, ми враховуємо найбільш поширені підходи.

Пов'язаність. У великих даних інформація про особу часто зберігається в кількох незалежних джерелах. Тому важливим аспектом є здатність з'єднувати записи, що належать одній особі або схожим особам. Враховуючи захист конфіденційності, дані, зібрані певним джерелом, мають бути анонімізовані перед їх публікацією. Проте незалежна анонімізація може обмежувати можливість об'єднання даних, що суттєво зменшує обсяг аналізів, які можуть бути проведені, а отже, і знання, що можна отримати з цих даних. Кількість можливих зв'язків, які можна створити відповідно до моделі конфіденційності, визначає, чи можна аналітику з'єднувати анонімізовані записи, що належать одній особі. Важливо зазначити, що з'єднуючи записи, які належать одній людині, ми збільшуємо кількість інформації про неї.

Композиційні властивості важливі для забезпечення збереження гарантій конфіденційності моделі в контексті великих даних. У таких даних процес збору не є централізованим, а розподілений серед численних джерел. Якщо одне з джерел даних надає перевагу конфіденційності та вирішує використовувати певну модель захисту даних, ці гарантії повинні зберігатися хоча б частково після об'єднання даних. Композиційність можна оцінювати як між випусками даних, що відповідають одній моделі конфіденційності, так і між випусками даних, що відповідають різним моделям, або між анонімізованими даними та необробленими даними.

Насамкінець, важливість зв'язку є критичною, оскільки великі дані формуються шляхом об'єднання даних з різних джерел. Точніше, можливість

аналізу даних про одну й ту саму особу в різних наборах даних є ключовою для ефективного аналізу. Таким чином, модель конфіденційності для великих даних повинна дозволяти анонімізованим даним залишатися певним чином взаємозв'язаними.

2.2. Методи і способи захисту інформації

Зазвичай комп'ютерне обладнання захищається такими ж засобами, як і інше цінне або чутливе обладнання, наприклад, за допомогою серійних номерів, дверей, замків та сигналізацій. Однак захист інформації та доступу до системи здійснюється за допомогою інших методів, деякі з яких є досить складними.

Заходи безпеки, пов'язані з комп'ютерними даними та доступом до них, орієнтовані на чотири основні загрози:

- крадіжка даних, таких як державні військові секрети з комп'ютерів;
- вандалізм, наприклад, знищення даних за допомогою комп'ютерних вірусів;
- шахрайство, наприклад, коли співробітники банків спрямовують кошти на власні рахунки;
- порушення приватності, наприклад, незаконний доступ до захищених особистих фінансових чи медичних даних з великих баз даних.

Одним із найбільш розповсюджених способів захисту комп'ютерних систем від крадіжок, вандалізму, порушень приватності та інших несанкціонованих дій є електронне відстеження та реєстрація доступу користувачів до системи та їхньої діяльності. Зазвичай це досягається шляхом надання кожному користувачу унікального паролю для доступу до системи. Проте для ефективного захисту інформації необхідний комплексний підхід, що включає всі елементи інформаційної безпеки: організаційні, фізичні, апаратні, програмні та інші заходи. Важливо використовувати лише сертифіковані та перевірені методи, що відповідають державним стандартам. Створення надійної системи захисту інформації дозволяє автоматично відстежувати використання

паролів, фіксуючи доступ до файлів і даних. Іншими методами захисту є збереження даних на окремих носіях, наприклад, магнітних стрічках або дисках, що не підключені безпосередньо до комп'ютерної системи. Крім того, дані часто шифруються, що дає можливість розшифрувати їх лише тим, хто має відповідний ключ шифрування.

Впровадження політики безпеки вимагає налаштування захисних засобів, управління системами захисту та моніторингу їхньої ефективності. Кібербезпека відповідає за вирішення питань, пов'язаних із захистом інформації. Вона включає профілактичні методи для запобігання крадіжкам, компрометаціям чи атакам на інформацію. Це потребує усвідомлення можливих інформаційних загроз, таких як віруси та інші види шкідливого програмного забезпечення. Стратегії кібербезпеки включають управління користувачами, ризиками та інцидентами. Кібербезпека є широкою категорією, яка охоплює різноманітні апаратні та програмні технології, застосовувані на різних рівнях, зокрема для захисту особистих, корпоративних або урядових пристроїв та мереж.

План кібербезпеки є надзвичайно важливим для компаній, які працюють з чутливою інформацією. Політика безпеки інформаційних технологій визначає правила та процедури для осіб, які отримують доступ до ресурсів організації. Ефективна політика безпеки є відображенням організаційної культури, де правила і процедури формуються на основі підходу співробітників до обробки та використання інформації. Тому така політика повинна бути адаптована до конкретної організації, враховуючи її співробітників, рівень ризику, сприйняття і цінність інформації, а також доступ, який вони мають. Ось чому багато компаній вважають політику безпеки малоефективною, якщо вона не відповідає реальним практикам використання та обміну інформацією в межах організації та ззовні.

Хешування — це процес поділу повідомлення на блоки, які зазвичай представлені у вигляді масивів, на підмножини з певними властивостями. Ці

властивості описуються хеш-функцією і називаються хеш-адресами. Для виконання зворотного процесу застосовуються хеш-таблиці, які забезпечують швидкий і точний доступ до елементів таблиці за хеш-адресами. В ідеальних умовах доступ до елемента відбувається за одне звернення, якщо хеш-адреса є унікальною. Однак у реальних умовах може статися так, що кілька елементів мають однакову хеш-адресу, що вимагає використання компромісних підходів для реалізації алгоритму. Хешування також перетворює вхідне повідомлення у бітовий рядок фіксованої довжини, зазвичай за допомогою певної маски.

Найпоширенішим методом автентифікації є використання пароля. Цей процес полягає в введенні користувачем секретної фрази, яка відповідає попередньо визначеному ідентифікатору. Введена інформація порівнюється з еталонним паролем, що зберігається в спеціальній базі даних, яка повинна бути захищена за допомогою криптографічних перетворень. Після цього приймається рішення щодо автентичності користувача та надається доступ до інформаційних ресурсів на основі перевірки з таблицею розподілу прав доступу. Така автентифікація є простою та поширеною, але має суттєві недоліки через вразливість методів зберігання паролів.

Цифрові сертифікати

Цифровий сертифікат, також відомий як сертифікат відкритого ключа, використовується для встановлення зв'язку між правом власності на відкритий ключ та особою, яка його має. Ці сертифікати призначені для обміну відкритими ключами, які використовуються для шифрування та автентифікації. Цифрові сертифікати містять сертифікований відкритий ключ, який ідентифікує власника ключа, метадані, що стосуються самого сертифіката, а також цифровий підпис, створений емітентом сертифіката. Основними цілями інфраструктури відкритих ключів є поширення, автентифікація та відкликання цифрових сертифікатів, що дозволяють аутентифікувати публічні ключі.

Цифровий сертифікат є документом, який підтверджує відповідність між відкритим публічним ключем та інформацією, що ідентифікує його власника.

Криптографія відкритого ключа базується на використанні пари ключів: приватного ключа, який зберігається у власника і використовується для підпису та розшифровки, та відкритого ключа, який застосовується для шифрування даних, що надсилаються власнику ключа, або для автентифікації даних, підписаних власником сертифіката. Цифровий сертифікат дозволяє учасникам обміну інформацією безпечно ділитися відкритим ключем, забезпечуючи їх автентифікацію.

Ці сертифікати підтримуються всіма основними веб-браузерами та серверами, забезпечуючи гарантію, що опублікований вміст не був змінений несанкціонованими особами, а також здійснюють обмін ключами для шифрування та розшифрування веб-контенту. Окрім цього, цифрові сертифікати використовуються в різних контекстах, як в Інтернеті, так і в оффлайн-режимі, для забезпечення криптографічної безпеки та конфіденційності даних.

Криптографія відкритого ключа забезпечує виконання різноманітних функцій, включаючи шифрування та автентифікацію. Однією з таких функцій є цифровий підпис, який створюється за допомогою алгоритмів підпису даних. Ці підписи дозволяють отримувачу безпомилково підтвердити, що дані були підписані власником певного відкритого ключа.

Цифровий підпис генерується шляхом хешування підписуваних даних за допомогою одностороннього криптографічного хешу. Потім отриманий хеш шифрується приватним ключем підписувача. Цей підпис містить зашифрований хеш, який можна перевірити, використовуючи відкритий ключ відправника для дешифрування підпису і повторного виконання того самого хешування на підписаному вмісті. Якщо два хеші співпадають, це підтверджує, що дані не були змінені з моменту підписання і що відправник володіє парою відкритих ключів, використаних для підпису.

Цифровий підпис зазвичай базується на розповсюдженні відкритого ключа через цифровий сертифікат, хоча це не є обов'язковим. Проте цифрові

сертифікати завжди підписуються цифровим способом, і їм не можна довіряти, якщо підпис не перевіряється. Існують три основні типи цифрових сертифікатів, які використовуються веб-серверами та браузерами для аутентифікації через Інтернет. Ці сертифікати прив'язують веб-сервер домену до фізичної або юридичної особи, яка володіє доменом. Такі сертифікати часто називають SSL-сертифікатами, хоча протокол SSL був замінений на TLS (протокол безпеки транспортного рівня).

— Сертифікати DV SSL, які підтверджують лише право на використання домену, забезпечують найменший рівень впевненості щодо власника сертифіката. Для отримання цих сертифікатів заявники мають лише довести, що мають право використовувати конкретне доменне ім'я. Хоча ці сертифікати гарантують безпечну передачу даних між сторонами, вони не підтверджують, хто є власником цього домену.

2.2 Висновки по розділу

Було проаналізовано уразливості інформаційних систем. Проведений аналіз уразливості інформаційно-комунікаційних систем показав, що існує значна кількість загроз які можуть привести до нанесення збитків при передачі інформації. Інформаційна безпека передачі даних в значній мірі залежить від реалізованого протоколу передачі даних, механізму передачі даних в мережі та комутаційного обладнання, що використовується в мережі. Але головну роль відіграє правильна політика безпеки яка включає нормативні постанови що до організаційного процесу.

Надзвичайно важливо виконувати організаційно-технічні заходи щодо зберігання ключів доступу та паролів, не зважаючи на фізичний рівень безпеки. Пароль – секретна фраза користувача, що використовується для його автентифікації та отримання доступу до сервісу. Він вимагає не менш надійного методу обробки та зберігання зі сторони серверу автентифікації для унеможливлення розсекречення та, відповідно, незаконного доступу до облікового запису, ніж на стороні користувача.

РОЗДІЛ 3 ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ

3.1. Створення середовища для виконання дипломної роботи

У першу чергу, було підготовлено середовище для виконання даної роботи: віртуальну машину з двома операційними системами: Windows 10 і Windows 7, а також сам персональний комп'ютер (ПК).

На ОС Windows 10 ми будемо реалізовувати проект, на Windows 7 – перевіriamo сумісність продукта, адже за статистикою – майже 23% усіх користувачів операційних систем використовують Windows 7, див. рис 3.1.

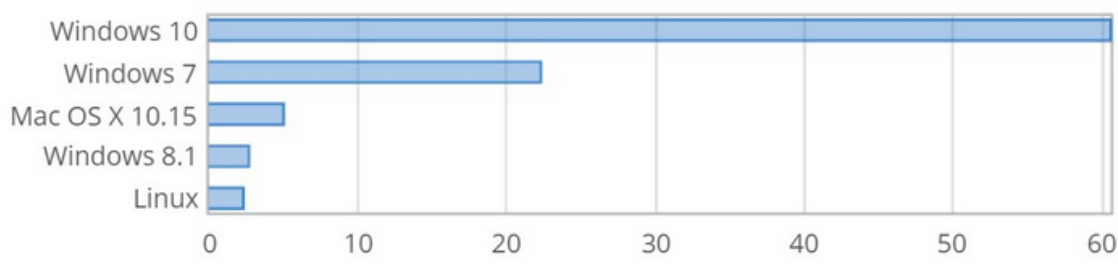


Рис.3.1. Популярність операційних систем

Для розгорнення декількох операційних систем на одній машині та їх адміністрування було використано гіпервізор, монітор віртуальної машини - VMware Workstation.

Гіпервізор, або монітор віртуальної машини, — це програмне або апаратне забезпечення, яке створює та керує віртуальними машинами. Комп'ютер, на якому працює гіпервізор і на якому запуснені одна або кілька віртуальних машин, називається хост-машиною, а кожна віртуальна машина — гостьовою машиною. Гіпервізор надає гостьовим операційним системам віртуальну платформу для роботи та контролює їх виконання. Окремі екземпляри різних операційних систем можуть одночасно використовувати віртуалізовані апаратні ресурси: наприклад, на одній фізичній машині x86 можуть працювати екземпляри Linux, Windows і macOS. Це відрізняється від віртуалізації на рівні операційної системи, де всі екземпляри, що зазвичай

називаються контейнерами, мають спільне ядро, хоча гостьові операційні системи можуть відрізнятися в користувацькому просторі (наприклад, різні дистрибутиви Linux з одним і тим самим ядром).

Використання технології гіпервізора зловмисними програмами та руткітами, які інсталиують себе як гіпервізор на рівні нижче операційної системи, відоме як гіперджекінг. Це може ускладнити виявлення таких загроз, оскільки зловмисне програмне забезпечення має змогу перехоплювати операції операційної системи, наприклад, коли користувач вводить пароль. Без спеціалізованих засобів для боротьби зі шкідливим ПО, його важко виявити, оскільки воно працює на рівні, нижчому за операційну систему. Одним з прикладів втілення цієї технології є лабораторний руткіт SubVirt, розроблений дослідниками Microsoft. Віртуальні машини, засновані на комп'ютерній архітектурі, забезпечують функціональність фізичного комп'ютера, і їх реалізація може включати як спеціалізоване обладнання, так і програмне забезпечення, або їх комбінацію.

VMware Workstation - це розміщений гіпервізор, який працює на x64 версіях операційних систем Windows та Linux, доступна версія x86 попередніх версій, він дозволяє користувачам налаштовувати віртуальні машини – VM на одній фізичній машині та використовувати їх одночасно разом із фактичною машиною. Кожна віртуальна машина може виконувати власну операційну систему, включаючи версії Microsoft Windows, Linux, BSD та MS-DOS. Робоча станція VMware розроблена VMware, Inc., підрозділом Dell Technologies. Існує безкоштовна версія VMware Workstation Player для некомерційного використання. Для використання фірмових операційних систем, таких як Windows, потрібна ліцензія на операційні системи. Готові віртуальні машини Linux, створені для різних цілей, доступні без ліцензії.

VMware Workstation Pro може в будь-який момент зберегти стан віртуальної машини. Після чого, пізніше відновити, фактично повернувши

віртуальну машину до збереженого стану, як вона була, і звільнитись від будь-яких помилок.

VMware Workstation включає можливість групування декількох віртуальних машин у папці інвентаризації. Потім машини в такій папці можуть бути включені та вимкнені як єдиний об'єкт, корисний для тестування складних середовищ клієнт-сервер.

3.2. Visual Studio - інтегроване середовище розробки ПЗ.

Microsoft Visual Studio — це інтегроване середовище розробки (IDE), розроблене компанією Microsoft. IDE — це програмне забезпечення, яке надає програмістам широкий набір інструментів для створення програмного забезпечення. Visual Studio використовується для розробки комп'ютерних програм, а також для створення вебсайтів, вебдодатків, вебслужб і мобільних додатків. Це середовище підтримує платформи Microsoft для розробки програмного забезпечення, такі як API Windows, Windows Forms, Presentation Foundation, Windows Store та Microsoft Silverlight. Visual Studio може працювати з як власним, так і керованим кодом.

У Visual Studio є вбудований редактор коду, який підтримує підсвічування синтаксису та автозавершення коду з підказками для змінних, функцій, методів, циклів і запитів. Ця функція доступна для XML та всіх мов програмування, які підтримуються IDE. Автозаповнення пропозицій відображається у вигляді списку поруч з курсором у вікні редактора коду.

Редактор коду Visual Studio також підтримує налаштування закладок у коді для швидкої навігації. Інші навігаційні засоби включають збір блоків коду та поступовий пошук, на додаток до звичайного пошуку тексту та пошуку в регулярних виразах. Редактор коду також включає буфер обміну для багатьох предметів та список завдань. Редактор коду підтримує фрагменти коду, які

зберігаються в шаблонах для повторюваного коду і можуть бути вставлені в код і налаштовані під проект, над яким працює. Також вбудований інструмент управління фрагментами коду. Ці інструменти з'являються у вигляді плаваючих вікон, які можна встановити для автоматичного приховування, коли вони не використовуються або стикуються на стороні екрана.

Visual Studio має компіляцію фоновому режим. Коли код пишеться, Visual Studio компілює його у фоновому режимі, щоб надати зворотній зв'язок про синтаксис та помилки компіляції, які позначені червоним хвилястим підкресленням. Попередження позначені зеленим підкресленням. Фонова компіляція не генерує виконуваний код, оскільки для нього потрібен інший компілятор, ніж той, який використовується для створення виконуваного коду.

На даний час Visual Studio підтримує : HTML / XHTML, JavaScript, XML / XSLT ,CSS, Python і Ruby. Також має вбудовані мови програмування:

- C / C ++ ;
- C # ;
- F # ;
- VB.NET.

Обрані алгоритми шифрування

Алгоритм AES

AES — це симетричний шифр, що означає використання одного і того ж ключа як для шифрування, так і для розшифрування даних.

Асиметричні системи шифрування вирішують цю проблему, застосовуючи відкритий ключ для захисту даних, який доступний усім. Розшифрувати ці дані може лише отримувач, який має відповідний приватний ключ. Такий підхід робить асиметричне шифрування більш ефективним для захисту даних під час їх передачі, оскільки відправник не потребує доступу до приватного ключа одержувача.

Таким чином, симетричні шифри, як AES, набагато ефективніше забезпечують захист даних у спокої, наприклад, коли вони зберігаються на жорсткому диску. Вони перевершують асиметричні шифри в таких випадках, оскільки:

— Симетричні шифри потребують значно менше обчислювальних ресурсів, що робить процес шифрування та дешифрування даних набагато швидшим порівняно з асиметричними шифрами. У перспективі симетричні шифри часто згадуються як приблизно "в 1000 разів швидші" за асиметричні.

— Завдяки своїй швидкості, симетричні шифри є набагато ефективнішими для шифрування великих обсягів даних. Асиметричні шифри, наприклад RSA, зазвичай використовуються лише для шифрування невеликих обсягів інформації, таких як ключі для захисту симетричного шифрування.

AES вважається одним із найнадійніших симетричних шифрів, які коли-небудь були розроблені. Існують і інші високозахищені симетричні шифри, такі як Twofish, спільно розроблений відомим криптографом Брюсом Шнайєром.

Правильно реалізований AES пом'якшує атаки бічних каналів, запобігаючи можливим шляхам витікання даних, саме там допомагає використання апаратного набору інструкцій AES, та за допомогою методів рандомізації для усунення зв'язку між захищеними шифром даними та будь-якими протікаючими даними.

Фактичний шифр AES потім виконує ряд математичних перетворень, використовуючи простий текст і секретний ключ як вихідну точку. За таким алгоритмом:

— Змішування. Кожну ітерацію ключ поєднується з простим текстом за допомогою алгоритму додавання XOR див рис. 3.2.

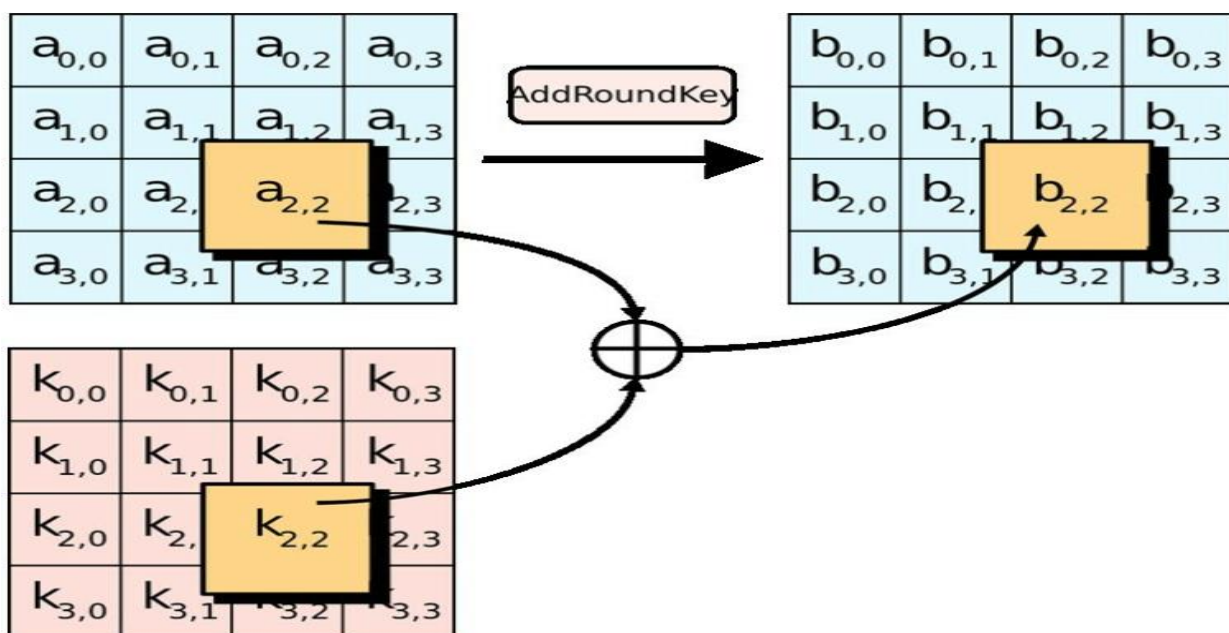


Рис. 3.2. Змішування алгоритма AES

— Заміна отриманих даних за допомогою таблиці заміщення. Цей крок в принципі дуже схожий, але декілько набагато складніший на практиці, із замінами шифрами, наприклад, Цезаря. Детальніше див. рис. 3.3.

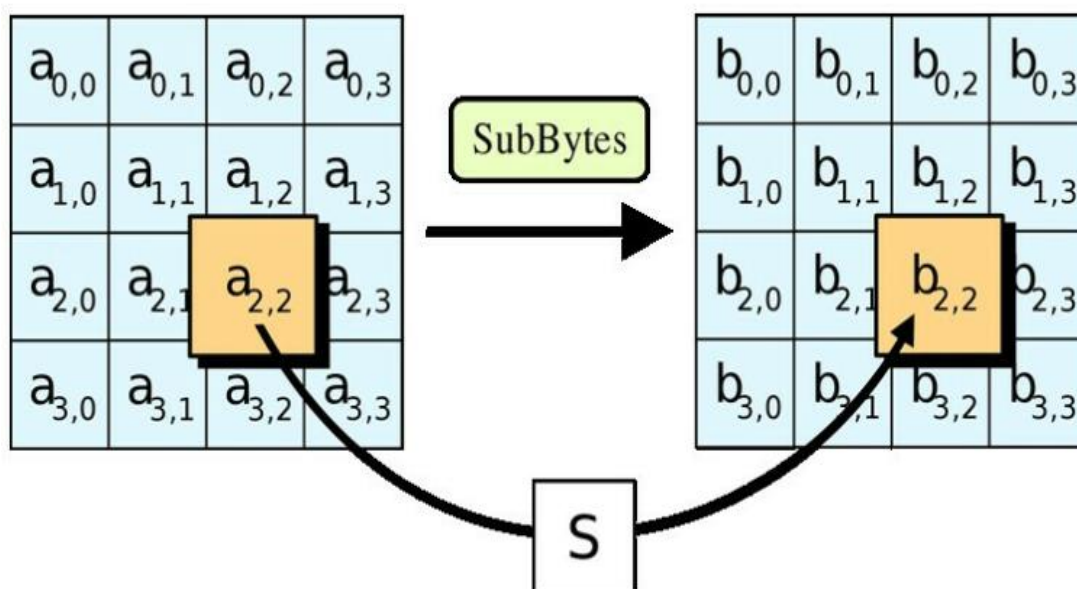


Рис. 3.3. Алгоритм заміни

— Змішування стовпців. До кожного стовпця застосовується подальший алгоритм, див. рис 3.4..

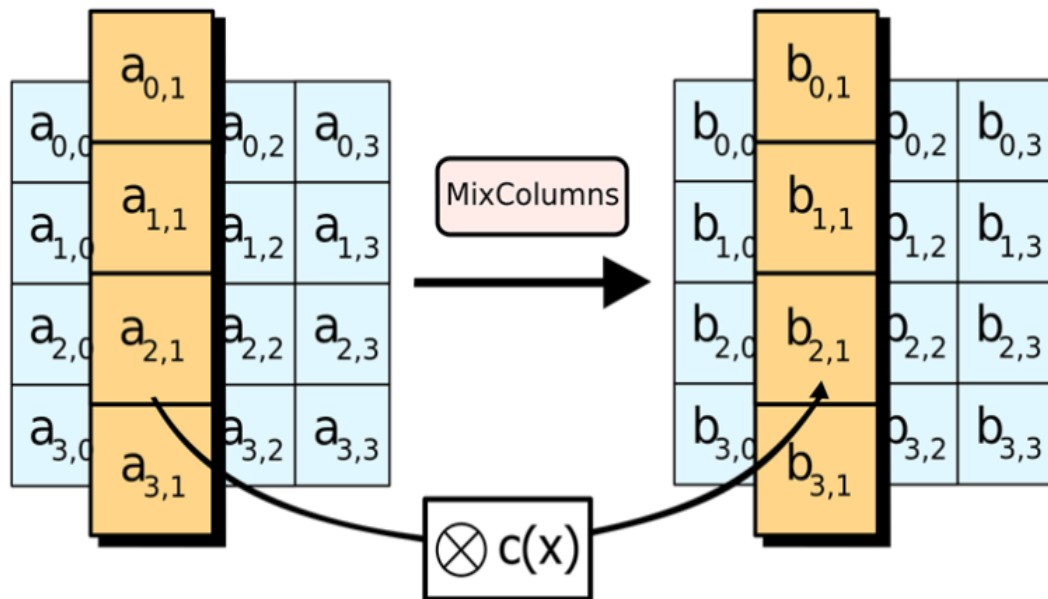


Рис. 3.4. Алгоритм змішування стовпців

Процес повторюється кілька разів, причому кожне повторення називається раундом. Кожен раунд повторно шифрується за допомогою одного із отриманих ключів під час розширення ключа.

Розшифрувати AES досить просто – для цього необхідно перепройти всі вищезазначені кроки, починаючи з кінця. Звичайно потрібно мати оригінальний секретний ключ.

Інтерфейс програми

Головне вікно дипломного проекту виглядає, як на рис. 3.5.:

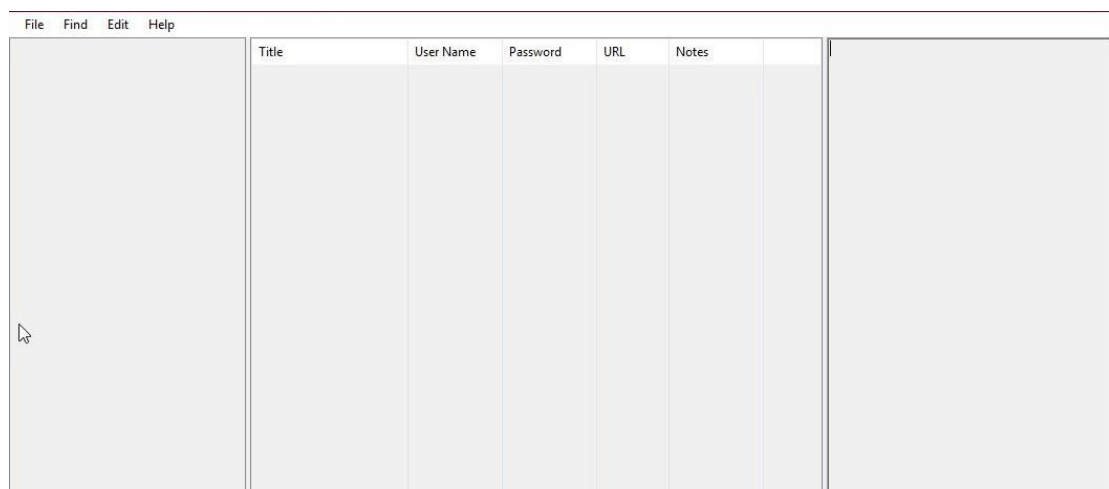


Рис.3.5. Головне вікно програми

У меню, яке знаходиться зліва у горі знаходяться випадаючі списки . File

– меню редагування та створення нових баз даних, Find – пошук у проекті, Edit – редагування збереженої інформації у базі, створення нових записів, редагування груп, Help – відомості про проект. Нижче наведені рис. із розгорнутими меню інформують про подальші дію в проекті

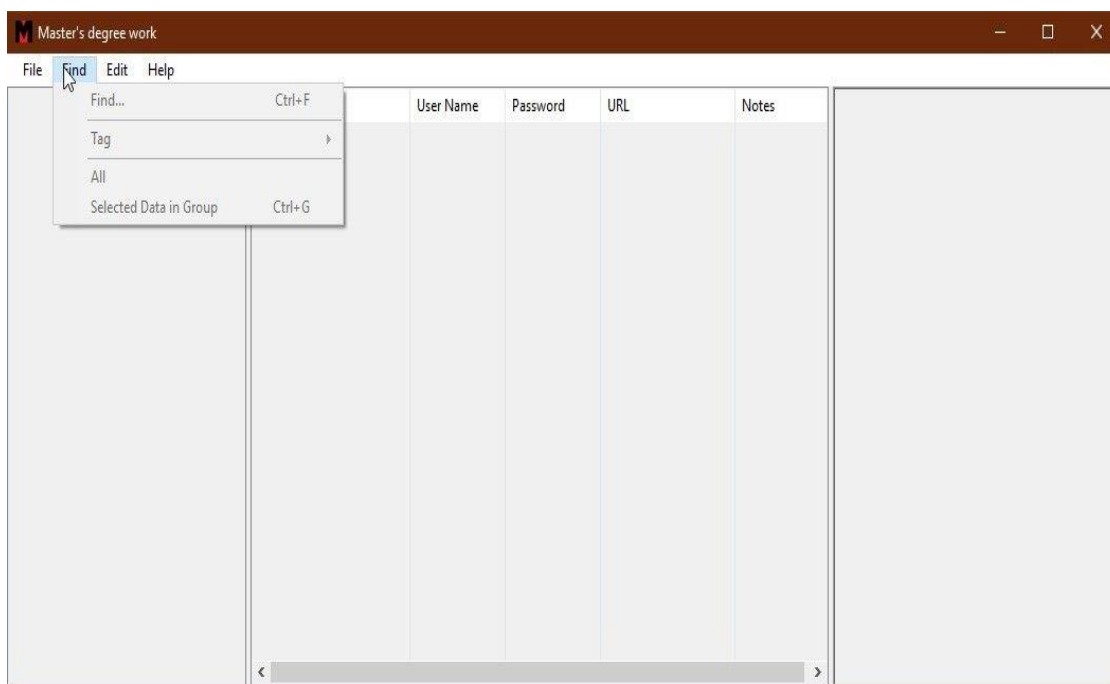


Рис. 3.6. Find

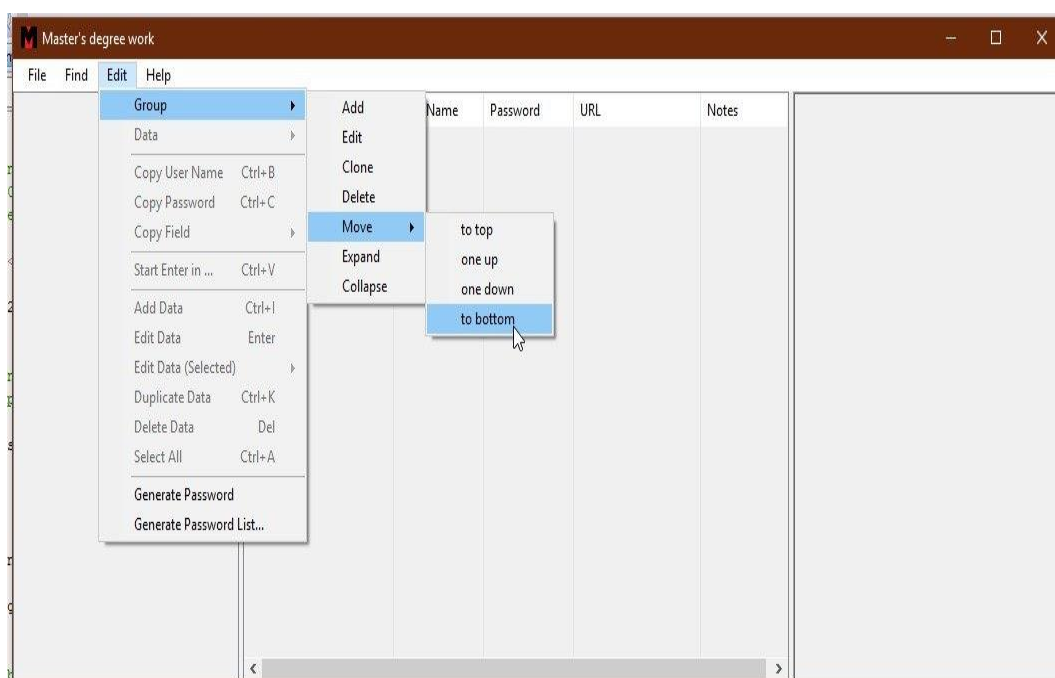


Рис. 3.7. Edit

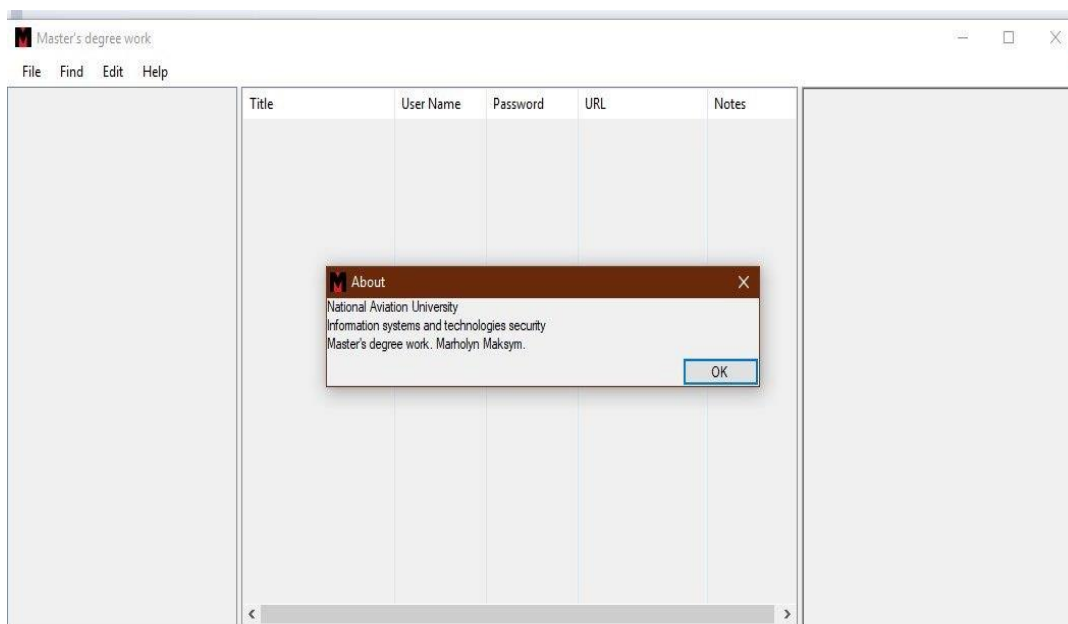


Рис 3.8. About

При створенні нової бази даних через меню File -> New відкривається вікно зберігання, де необхідно вказати шлях по якому зберігатись файл.

Усі файли проекту мають розширення MYMAX. Після вибору місця зберігання проекту необхідно вказати пароль та обрати назву бази даних – рис. 3.9. Також користувач має можливість інтерактивно змінювати ступінь безпеки за яким шифруються файли, але усе залежить від швидкодії машини на якій запускається проект – на слабкому комп'ютері відкриття та редагування складних алгоритмів займає більше часу.

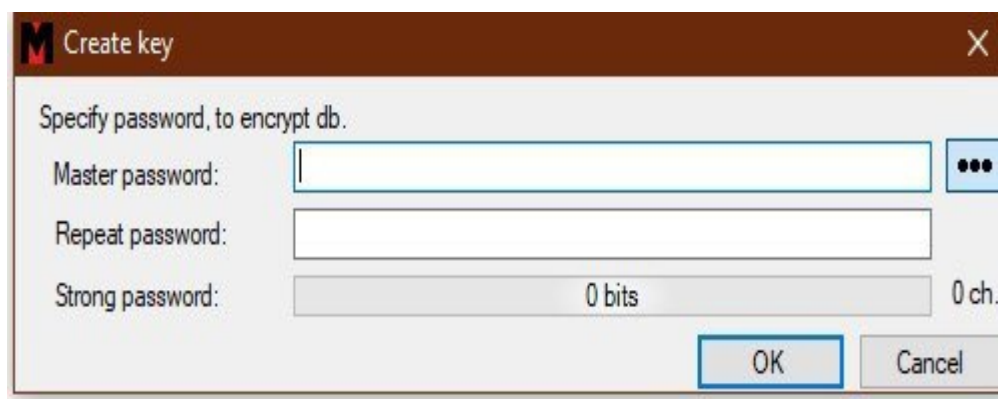


Рис 3.9. Pass

Стійкість алгоритму залежить від надійності ключа шифрування, саме тому було введено перевірку надійності паролю, у строчці “Strong Password”, як

зображено на рис. 3.10.:

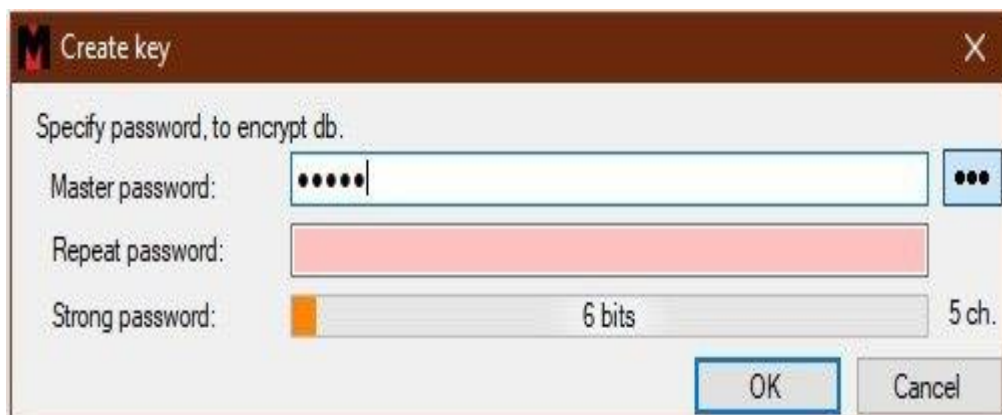
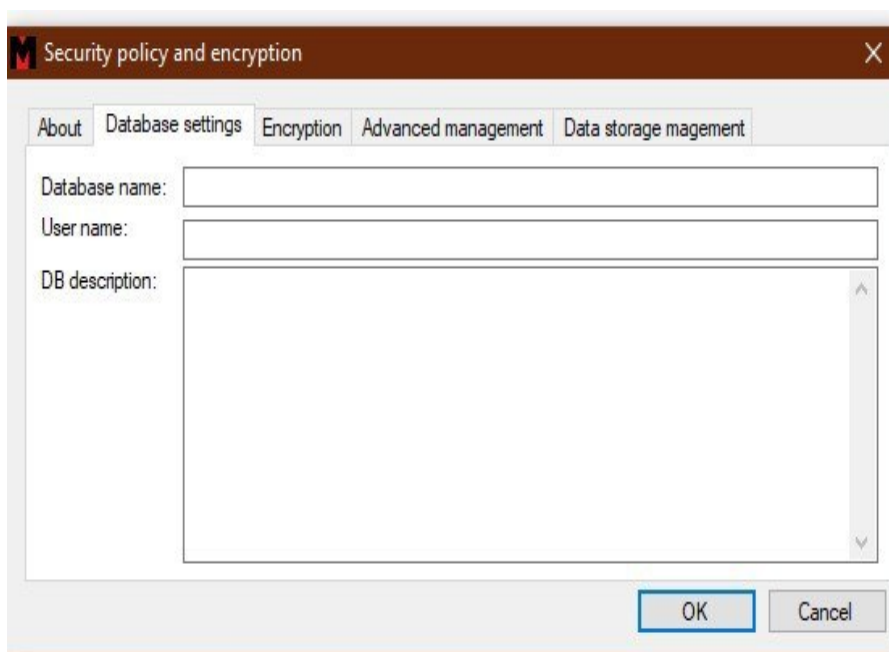


Рис 3.10. Strong Password

Після вибору та введення пароля відкривається наступне вікно, яке надає можливість скорегувати політику безпеки та спосіб захисту програми. Дуже важливо щоб користувач заздалегідь знав за що відповідає та чи інша функція.

У наступній вкладинці “Database settings” знаходиться меню редагування основних даних захищеної бази даних. У ній є можливість створити опис, надати назву але це не є обов’язковим. На рис. 3.11. відображене меню введення опису та назви нової бази даних.



У вкладинці “Encryption” користувач має можливість обрати алгоритм шифрування, стійкість та надійність методів захисту бази даних, які можливо

гнучко скоректувати залежно від стандартів інформаційної безпеки яким необхідно слідувати. Але як правило не усі комп'ютери однаково швидко виконують криптографічні перетворення. Існують різні комп'ютери для різних типів задач, адже якщо заплановано використовувати машину для тільки у браузері для друкування та перегляду інтернет сторінок – то усі обчислення відбуваються не на стороні клієнта, а на хмарному сервері, отже і комп'ютер не повинен бути із великою обчислювальною спроможністю, для такого типу задач. З іншої сторони, якщо комп'ютер призначений для створення та редагування 3D – графіки, розробки складних креслень, обрахування інженерних формул та обрахування складних математичних, фізичних формул – то комп'ютер повинен мати спроможність обраховувати такі данні швидко. Адже час це гроші. Саме тому виникають дуже великі прірви між різними типами комп'ютерів. Тому дуже важливо мати змогу гнучко редагувати та створювати необхідні політики безпеки у середині програми, та мати інструменти для аналізу криптографічних перетворень на тій чи іншій машині. То що завжди є залежність від часу та надійності шифрування. На різних машинах на одну секунду може обрахуватись різна кількість ітерацій шифрування.

У меню “Key Settings” відбувається збільшення введеного ключа за допомогою функцій девіації. Завдяки гнучкій функції редагування кількості ітерацій функції девіації програма надає можливість користувачу налаштувати максимально допустиме значення, опираючись на ресурси комп'ютера. Завдяки кнопкам “Check algorithm speed”, рис. 3.14., користувач може перевірити скільки займає обрахування зазначеної кількості ітерацій. Але знову ж таки постає проблема підбору максимально ефективного значення ітерацій функції девіації.

Також можливо використовувати додаткове перетворення Argon2, що працює за таким алгоритмом:

— Хешує пароль пароль ;

- Результат хешування записується блоками в пам'ять ;
- Блоки пам'яті перетворюються за допомогою функції стиснення ;
- В результаті роботи генерується ключ.

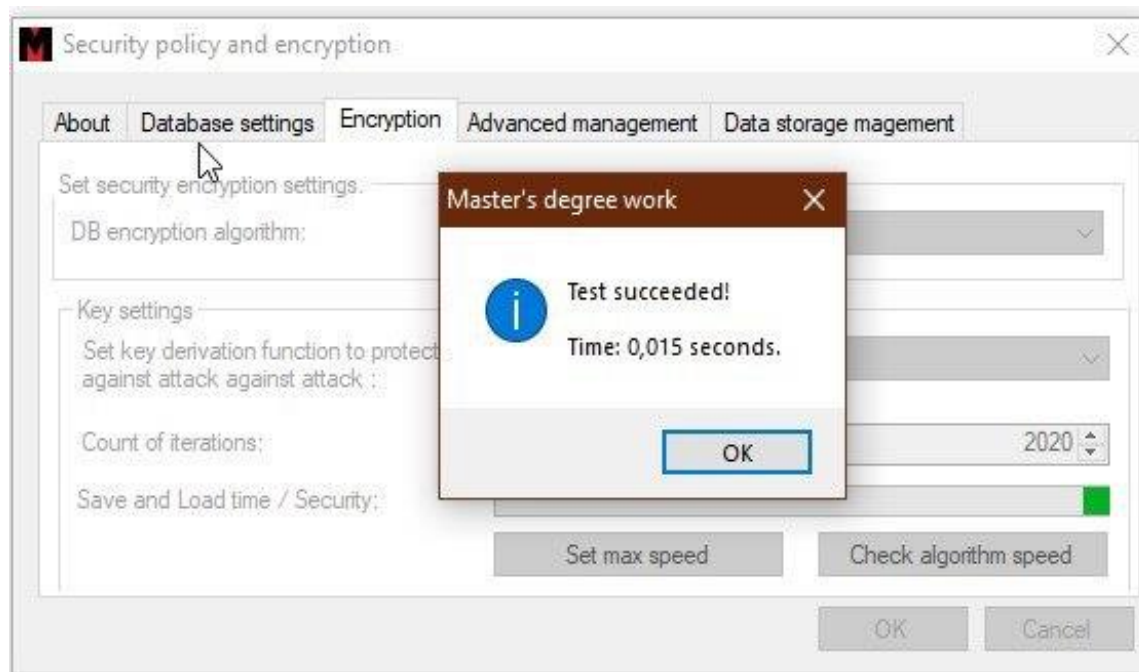


Рис 3.13. Check algorithm speed



Рис. 3.14. Set max speed

Вкладка “Advanced magement” надає можливість встановлювати політику безпеки. Вона передбачає зміну пароля через встановлений проміжок

часу у днях. Є дві опції за якими можливо нагадати користувачу о необхідності зміни пароля та примусово змінити його. Без цих опцій політика безпеки стає вразлива, так як виростає вірогідність, що пароль до бази даних стане відомий третім особам, рис. 3.15..



Рис. 3.15. Advanced magement

Для зручності редагування даних є можливість зберігати видалені файли у окремій групі, так званій “корзині”, користувачі ос Windows звикли до безпечного видалення даних через “корзину”, тому така функція реалізована у вкладниці “Data storage”, рис. 3.16.:

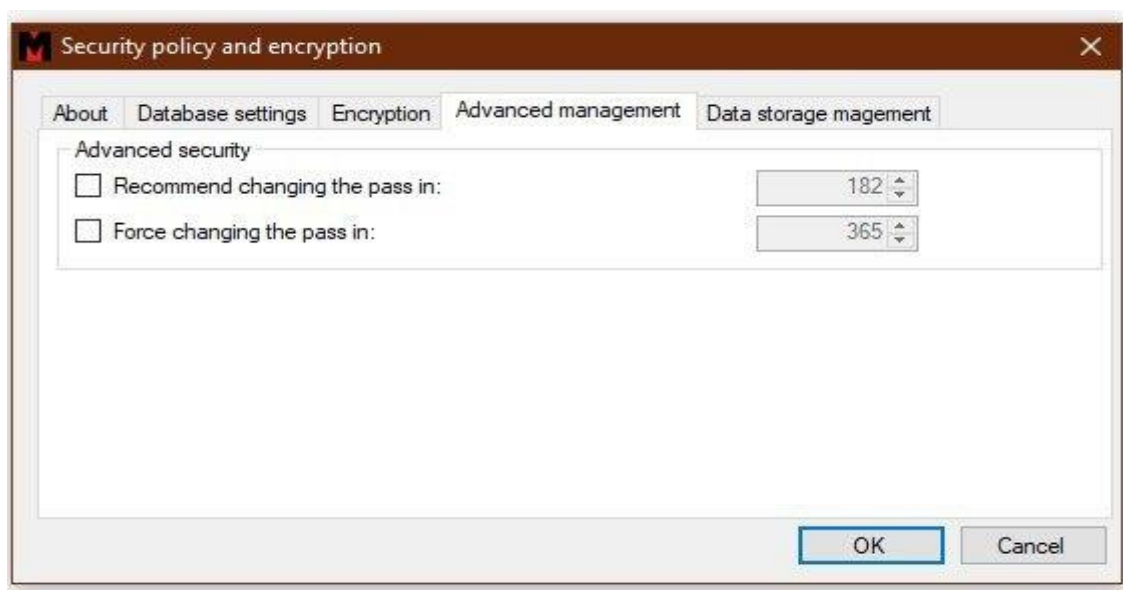


Рис. 3.16. Data storage

При завершенні створення початкового фалу проекту стануть активні вікна редагування бази даних. Поле ліворуч відповідає за створення та редагування груп, вони створенні для зручності використання програми. Поле по центру відповідає за редагування даних та створення нових записів.

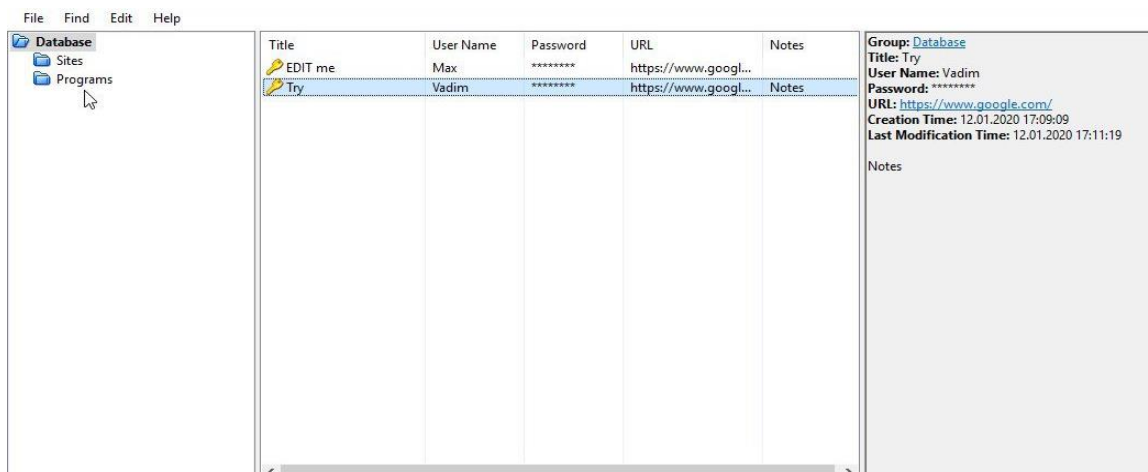


Рис. 3.17. Main window

Оцінка ефективності

В реалізованому проєкті вбудована функція оцінки ефективності захисту даних. В залежності від введеного паролю інтерактивно повідомлює що до надійності, виводить інформацію щодо його бітності та уількості символів.

Функція автоматичного введення екномить не тільки час на копіювання

чи набір паролей але й гарантує, що інформацію жоден злоумисник не зможе запам'ятати та відтворити. Критерії оцінки етапу проектування та експлуатації вказані в табл. 3.1 та 3.2.

Таблиця 3.1

Критерії оцінки ефективності на етапі проектування

Критерії етапу проектування		
Складність	Коректність	Трудоємність
<p>— Аналіз проблем захищеності сучасних інформаційних систем;</p> <p>— пошук та дослідження існуючих рішень в сферах запобігання витоку персональних та конфіденційних даних;</p> <p>— вибір методології для розробки пз;</p> <p>— розробка алгоритмів та логіки на яких буде реалізован програмне забезпечення;</p>	<p>— Відповідність до існуючих нормативно правових актах інформаційної безпеки;</p> <p>— Реалізація усіх засад обраних методів захисту інформації.</p>	<p>— Вивчення сучасних методів та роботи з обраним середовищем розробки програмного забезпечення.</p> <p>— Оновлення знань нормативно правових актах інформаційної безпеки України.</p>

Таблиця 3.2

Критерії оцінки ефективності на етапі експлуатації

Критерії етапу експлуатації		
Складність	Коректність	Трудоємність
<p>— Розуміння інтерфейсу програмної</p>	<p>— Коректність вооду даних для</p>	<p>— Звикання до необхідності</p>

реалізації	зберігання та захисту у програмі.	використовувати новий програмний засіб інформаційної безпеки.
------------	-----------------------------------	---

3.3. Висновки по розділу

Був створений програмний продукт, який дозволяє зберігати конфіденційні записи, логіни та паролі, а також сортувати і редагувати їх через простий та зручний інтерфейс. Якщо розглянути сучасні програмні засоби для збереження ключів доступу до різноманітних ресурсів, то можна помітити кілька спільних рис. Більшість з них інтегровані у конкретні програми, такі як браузері чи спеціалізовані додатки, і включають функції автоматичного запам'ятовування логінів та паролів для швидкої аутентифікації. Інші ж рішення використовують копіювання паролів у буфер обміну через функції Windows. Однак такі методи не підходять у випадках, коли до одного комп'ютера мають доступ кілька користувачів або коли пристрій використовується у публічних місцях, де будь-хто може увійти під чужим збереженим паролем. Це абсолютно неприйнятно, особливо в умовах інформаційної війни, коли конфіденційна інформація може мати не лише фінансову, а й життєво важливу цінність.

Проаналізувавши існуючі методи, я розробив продукт, який удосконалює сучасні рішення у сфері зберігання конфіденційної та персональної інформації. Головною новацією стало автоматичне введення збережених і зашифрованих даних за допомогою віртуальної клавіатури — тепер не потрібно використовувати буфер обміну чи вручну вводити паролі. Достатньо натискання однієї клавіші, і програма автоматично введе логін і пароль. Для підтримки старих моделей комп'ютерів і підвищення рівня захисту користувач отримає вибір: швидке шифрування, яке займає мінімум часу, або ж більш надійний метод, що потребує додаткового часу для відкриття, редагування та збереження зашифрованих файлів. На мою думку, подібні рішення слід інтегрувати в операційні системи для покращення інформаційної безпеки.

СПИСОК БІБЛЮГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286).
2. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403).
3. Державний стандарт України «Захист інформації. Технічний захист. Інформації. Основні положення». Чинний від 01.01.1997 р.
4. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».
5. Brookman J, Hans GS – Why collection matters: surveillance as a de facto privacy harm. In: Big data and privacy: making ends meet. The center for internet and society – 2019 – Stanford Law School.Закон України «Про Національну систему конфіденційного зв'язку» » // Відомості Верховної Ради України (ВВР) – 2002. – №22. ст.816 (остання редакція від 19.04.2014).
7. Закон України «Про захист інформації в Інформаційно-телекомунікаційних системах» » // Відомості Верховної Ради України (ВВР) – 1994. – №31. ст.286 (остання редакція від 27.03.2014).
8. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – [Чинний від 01.01.1997]. – Держспоживстандарт України, 2006, №4233, 18 с. – (Національні стандарти України).
9. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. – [Чинний від 01.01.1998]. – Держспоживстандарт України, 2007, №4233, 32 с. – (Національні стандарти України).
10. Конституція України від 28.06.1996 №254к/96-ВР – 1996. №30. – С.141.(остання редакція від 20.04.2018).
11. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в

комп'ютерних системах від несанкціонованого доступу. – 1999. – №22. – С.20(із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 №806).

12. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – 1999. – №22.

13. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. – 2007. – №232. – С.6(із змінами згідно наказу Адміністрації Держспецзв'язку від 03.11.2011 №93/ДСК).

14. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. – 2000. – №53. – С.32(із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 №806).

15. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – 1999. – №22. – С.74(із змінами згідно наказу Адміністрації Держспецзв'язку від 15.10.2008 №172).

16. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Правила № 373). – 2006. – №373 – с. 10.

17. From Cyber-Bombs to Political fallout: threat Representations with an impact in Cyber-Security Discourse. International Studies Review: [Електронний ресурс]. – Режим доступу до статті: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200862.

18. Cyber Security is a Board Level Issue: [Електронний ресурс]. – Режим доступу до статті: <https://www.crowdstrike.com/blog/why-cybersecurity-should-be-a-board-level-discussion>.

19. Cybersecurity: A Pre-history: [Електронний ресурс]. – Режим доступу до статті: <https://www.tandfonline.com/doi/abs/10.1080/02684527.2012.708530>.

20. An Investigation on Cyber Security Threats and Security Models: [Електронний ресурс]. – Режим доступу до статті:

<https://www.semanticscholar.org/paper/An-Investigation-on-Cyber-Security-Threats-and-Thakur-Qiu/26534add8408c3b1517777026cc3d19430a8727a>

21. Implementation of efficient AES encryption: [Електронний ресурс]. – Режим доступу до статті: https://www.researchgate.net/publication/308866491_FPGA_implementation_of_efficient_AES_encryption

22. Various Schemes for Database Encryption: [Електронний ресурс]. – Режим доступу до статті: https://www.ripublication.com/ijaer17/ijaerv12n19_104.pdf

Додаток А

```

import tkinter as tk
from tkinter import ttk, messagebox, filedialog, simpledialog
from cryptography.fernet import Fernet
import secrets
import random
import threading
import pyperclip
import string
import time
import os
import hashlib
import re

class AdvancedMatrixBackground(tk.Canvas):
    """Клас для створення анімованого фону у стилі матриці."""
    def __init__(self, master, **kwargs):
        super().__init__(master, **kwargs)

        self.chars = list('ABCDEFGHIJKLMNOPQRSTUVWXYZабвгдеєжзиййклмнопрстуфхцчшщью
я0123456789!@#$%^&*()_+')

        self.drops = []
        self.speed = []
        self.configure(bg='black', highlightthickness=0)
        self.setup_matrix()

    def setup_matrix(self):

```

```

"""Підготовка матриці з випадковими параметрами руху символів."""
width = self.wininfo_screenwidth()
height = self.wininfo_screenheight()
column_count = width // 15

for _ in range(column_count):
    self.drops.append(random.randint(-50, height))
    self.speed.append(random.uniform(0.5, 2.0))

self.start_matrix_animation()

def start_matrix_animation(self):
    """Запуск анімації матриці в окремому потоці."""
    def animate():
        while True:
            self.update_matrix()
            time.sleep(0.05)

    thread = threading.Thread(target=animate, daemon=True)
    thread.start()

def update_matrix(self):
    """Оновлення матриці з динамічними символами."""
    width = self.wininfo_screenwidth()
    height = self.wininfo_screenheight()
    column_count = width // 15

    self.delete('all')

```

```

for i in range(column_count):
    char = random.choice(self.chars)
    color_intensity = random.randint(100, 255)
    color = f'#00{hex(color_intensity)[2:]}00'

    self.create_text(
        i * 15,
        self.drops[i],
        text=char,
        fill=color,
        font=('Courier', 14, 'bold')
    )

    self.drops[i] += self.speed[i]

    if self.drops[i] > height:
        self.drops[i] = random.randint(-50, 0)
        self.speed[i] = random.uniform(0.5, 2.0)

    self.update()

```

```

class UltraSecureEncryptionApp:
    """Головний клас додатку для шифрування та безпеки."""
    def __init__(self, master):
        self.master = master
        master.title(" Криптографічний Менеджер")
        master.geometry("1200x800")
        master.configure(bg='black')

```

Кольорова палітра

```
self.colors = {
    'bg': '#121212',
    'text': '#00FF7F',
    'accent': '#00AA00',
    'input_bg': '#1E1E1E'
}
```

Створення матричного фону

```
self.matrix_bg = AdvancedMatrixBackground(
    master,
    width=master.winfo_screenwidth(),
    height=master.winfo_screenheight()
)
self.matrix_bg.place(x=0, y=0)
```

Ініціалізація змінних

```
self.encryption_key = None
self.encrypted_history = []
self.decrypted_history = []
self.saved_passwords = {}
self.secure_notes = {}
```

Створення головного інтерфейсу

```
self.create_main_interface()
```

```
def create_main_interface(self):
```

"""Створення головного інтерфейсу додатку."""

```
main_frame = tk.Frame(self.master, bg=self.colors['bg'])
```

```
main_frame.pack(fill=tk.BOTH, expand=True, padx=20, pady=20)
```

```
self.notebook = ttk.Notebook(main_frame)
```

```
self.notebook.pack(fill=tk.BOTH, expand=True)
```

```
tabs = [
```

```
    ("Шифрування", self.create_encryption_tab),
```

```
    ("Дешифрування", self.create_decryption_tab),
```

```
    ("Менеджер Паролів", self.create_password_manager_tab),
```

```
    ("Безпечні Нотатки", self.create_secure_notes_tab),
```

```
("Аналіз Безпеки", self.create_security_analysis_tab)
```

```
]
```

```
for title, creator in tabs:
```

```
    tab = ttk.Frame(self.notebook)
```

```
    self.notebook.add(tab, text=title)
```

```
    creator(tab)
```

```
def create_encryption_tab(self, tab):
```

```
    """Створення вкладки шифрування."""
```

```
    input_label = tk.Label(tab, text="Введіть текст для шифрування:",
```

```
                           bg=self.colors['bg'], fg=self.colors['text'],
```

```
                           font=('Courier', 14))
```

```
    input_label.pack(pady=10)
```

```
    input_text = tk.Text(tab, height=10, width=70,
```

```
                        bg=self.colors['input_bg'],
```

```
                        fg=self.colors['text'],
```

```
                        font=('Courier', 12))
```

```
input_text.pack(pady=10)
```

```
btn_frame = tk.Frame(tab, bg=self.colors['bg'])
```

```
btn_frame.pack(pady=10)
```

```
buttons = [
```

```
    ("Зашифрувати", lambda: self.encrypt_text(input_text)),
```

```
    ("Копіювати", lambda: self.copy_to_clipboard(input_text)),
```

```
    ("Зберегти", lambda: self.save_encrypted_file(input_text))
```

```
]
```

```
for text, command in buttons:
```

```
    btn = tk.Button(btn_frame, text=text, command=command,
```

```
                    bg=self.colors['accent'], fg=self.colors['text'])
```

```
    btn.pack(side=tk.LEFT, padx=5)
```

```
def create_decryption_tab(self, tab):
```

```
    """Створення вкладки дешифрування."""
```

```
    input_label = tk.Label(tab, text="Введіть зашифрований текст:",
```

```
                           bg=self.colors['bg'], fg=self.colors['text'],
```

```
                           font=('Courier', 14))
```

```
    input_label.pack(pady=10)
```

```
    input_text = tk.Text(tab, height=10, width=70,
```

```
                        bg=self.colors['input_bg'],
```

```
                        fg=self.colors['text'],
```

```
                        font=('Courier', 12))
```

```
    input_text.pack(pady=10)
```

```
btn_frame = tk.Frame(tab, bg=self.colors['bg'])
```

```
btn_frame.pack(pady=10)
```

```
buttons = [
```

```
    ("Розшифрувати", lambda: self.decrypt_text(input_text)),
```

```
    ("Копіювати", lambda: self.copy_to_clipboard(input_text))
```

```
]
```

```
for text, command in buttons:
```

```
    btn = tk.Button(btn_frame, text=text, command=command,
```

```
                    bg=self.colors['accent'], fg=self.colors['text'])
```

```
    btn.pack(side=tk.LEFT, padx=5 )
```

```
def create_password_manager_tab(self, tab):
```

```
    """Створення вкладки менеджера паролів."""
```

```
    input_label = tk.Label(tab, text="Введіть назву сайту:",
```

```
                           bg=self.colors['bg'], fg=self.colors['text'],
```

```
                           font=('Courier', 14))
```

```
    input_label.pack(pady=10)
```

```
    site_entry = tk.Entry(tab, width=50, bg=self.colors['input_bg'],
```

```
                           fg=self.colors['text'], font=('Courier', 12))
```

```
    site_entry.pack(pady=10)
```

```
    password_label = tk.Label(tab, text="Введіть пароль:",
```

```
                              bg=self.colors['bg'], fg=self.colors['text'],
```

```
                              font=('Courier', 14))
```

```
    password_label.pack(pady=10)
```

```

password_entry = tk.Entry(tab, width=50, bg=self.colors['input_bg'],
                           fg=self.colors['text'], font=('Courier', 12))
password_entry.pack(pady=10)

btn_frame = tk.Frame(tab, bg=self.colors['bg'])
btn_frame.pack(pady=10)

save_btn = tk.Button(btn_frame, text="Зберегти",
                     command=lambda: self.save_password(site_entry.get(),
password_entry.get()),
                     bg=self.colors['accent'], fg=self.colors['text'])
save_btn.pack(side=tk.LEFT, padx=5)

view_btn = tk.Button(btn_frame, text="Переглянути паролі",
                     command=self.view_passwords,
                     bg=self.colors['accent'], fg=self.colors['text'])
view_btn.
pack(side=tk.LEFT, padx=5)

def create_secure_notes_tab(self, tab):
    """Створення вкладки захищених нотаток."""
    input_label = tk.Label(tab, text="Введіть заголовок нотатки:",
                           bg=self.colors['bg'], fg=self.colors['text'],
                           font=('Courier', 14))
    input_label.pack(pady=10)

    title_entry = tk.Entry(tab, width=50, bg=self.colors['input_bg'],
                           fg=self.colors['text'], font=('Courier', 12))
    title_entry.pack(pady=10)

```

```

note_label = tk.Label(tab, text="Введіть текст нотатки:",
                      bg=self.colors['bg'], fg=self.colors['text'],
                      font=('Courier', 14))
note_label.pack(pady=10)

note_text = tk.Text(tab, height=10, width=70,
                    bg=self.colors['input_bg'],
                    fg=self.colors['text'],
                    font=('Courier', 12))
note_text.pack(pady=10)

btn_frame = tk.Frame(tab, bg=self.colors['bg'])
btn_frame.pack(pady=10)

save_note_btn = tk.Button(btn_frame, text="Зберегти нотатку",
                          command=lambda: self.save_secure_note(title_entry.get(),
note_text.get("1.0", tk.END)),
                          bg=self.colors['accent'], fg=self.colors['text'])
save_note_btn.pack(side=tk.LEFT, padx=5)

view_notes_btn = tk.Button(btn_frame, text="Переглянути нотатки",
                           command=self.view_secure_notes,
                           bg=self.colors['accent'], fg=self.colors['text'])
view_notes_btn.pack(side=tk.LEFT, padx=5)

def create_security_analysis_tab(self, tab):
    """Створення вкладки аналізу безпеки."""
    analysis_label = tk.Label(tab, text="Аналіз безпеки паролів:",

```

```

        bg=self.colors['bg'], fg=self.colors['text'],
        font=('Courier', 14))
analysis_label.pack(pady=10)

analyze_btn = tk.Button(tab, text="Аналізувати паролі",
                        command=self.analyze_passwords,
                        bg=self.colors['accent'], fg=self.colors['text'])
analyze_btn.pack(pady=10)

def encrypt_text(self, text_widget):
    """Шифрування тексту."""
    text = text_widget.get("1.0", tk.END).strip()
    if not text:
        messagebox.showwarning("Увага", "Введіть текст для шифрування.")
        return
    self.encryption_key = Fernet.generate_key()
    cipher = Fernet(self.encryption_key)
    encrypted = cipher.encrypt(text.encode())
    messagebox.showinfo("Зашифровано", f"Зашифрований
    текст:\n{encrypted.decode()}")
    self.encrypted_history.append(encrypted.decode())

def decrypt_text(self, text_widget):
    """Дешифрування тексту."""
    text = text_widget.get("1.0", tk.END).strip()
    if not text or not self.encryption_key:
        messagebox.showwarning("Увага", "Введіть зашифрований текст або
згенеруйте ключ.")
        return

```

```

cipher = Fernet(self.encryption_key)
try:
    decrypted = cipher.decrypt(text.encode()).decode()
    messagebox.showinfo("Розшифровано", f"Розшифрований
текст:\n{decrypted}")
    self.decrypted_history.append(decrypted)
except Exception as e:
    messagebox.showerror("Помилка", "Не вдалося розшифрувати текст.
Перевірте правильність введення.")

```

```

def save_encrypted_file(self, text_widget):
    """Збереження зашифрованого тексту у файл."""
    text = text_widget.get("1.0", tk.END).strip()
    if not text:
        messagebox.showwarning("Увага", "Введіть текст для збереження.")
        return
    file_path = filedialog.asksaveasfilename(defaultextension=".txt",
        filetypes=[("Text files", "*.txt"), ("All files", "*.*)])
    if file_path:
        with open(file_path, 'w') as file:
            file.write(text)
        messagebox.showinfo("Збережено", "Файл успішно збережено.")

```

```

def copy_to_clipboard(self, text_widget):
    """Копіювання тексту в буфер обміну."""
    text = text_widget.get("1.0", tk.END).strip()
    if text:
        pyperclip.copy(text)
        messagebox.showinfo("Копійовано", "Текст скопійовано в буфер обміну.")

```

```

def save_password(self, site, password):
    """Збереження пароля для сайту."""
    if site and password:
        self.saved_passwords[site] = password
        messagebox.showinfo("Збережено", "Пароль успішно збережено.")
    else:
        messagebox.showwarning("Увага", "Введіть назву сайту та пароль.")

def view_passwords(self):
    """Перегляд збережених паролів."""
    if self.saved_passwords:
        passwords = "\n".join([f"{site}: {password}" for site, password in
self.saved_passwords.items()])
        messagebox.showinfo("Збережені паролі", passwords)
    else:
        messagebox.showinfo("Збережені паролі", "Паролі не знайдено.")

def save_secure_note(self, title, note):
    """Збереження захищеної нотатки."""
    if title and note:
        self.secure_notes[title] = note
        messagebox.showinfo("Збережено", "Нотатку успішно збережено.")
    else:
        messagebox.showwarning("Увага", "Введіть заголовок та текст
нотатки.")

def view_secure_notes(self):
    """Перегляд захищених нотаток."""

```

```

if self.secure_notes:
    notes = "\n".join([f"{title}: {note}" for title, note in self.secure_notes.items()])
    messagebox.showinfo("Захищені нотатки", notes)
else:
    messagebox.showinfo("Захищені нотатки", "Нотатки не знайдено.")

def analyze_passwords(self):
    """Аналіз паролів на складність."""
    if not self.saved_passwords:
        messagebox.showinfo("Аналіз безпеки", "Паролі не знайдено.")
        return
    weak_passwords = [site for site, password in self.saved_passwords.items() if
len(password) < 8]
    if weak_passwords:
        messagebox.showwarning("Аналіз безпеки", f"Слабкі паролі знайдено для
сайтів: {', '.join(weak_passwords)}")
    else:
        messagebox.showinfo("Аналіз безпеки", "Всі паролі є достатньо
складними.")

# Основний запуск додатку
if name == "__main__":
    root = tk.Tk()
    app = UltraSecureEncryptionApp(root)
    root.mainloop()

```

Додаток А

Актуальні методи захисту інформації в умовах інформаційної війни

Цей код створює багатофункціональний криптографічний додаток з графічним інтерфейсом на основі бібліотеки Tkinter.

Основна ідея полягає в тому, щоб об'єднати в одному додатку функції шифрування/дешифрування текстів, генерації паролів та збереження історії операцій.

Мета коду:

1. **Забезпечити зручний та інтуїтивно зрозумілий інтерфейс** для виконання криптографічних операцій.
2. **Реалізувати функції шифрування та дешифрування текстів** з використанням надійного алгоритму Fernet.
3. **Надати можливість генерації криптографічно стійких паролів** різної довжини.
4. **Забезпечити збереження історії** виконаних операцій для подальшого перегляду.
5. **Створити візуально привабливий інтерфейс** з використанням анімованого фону у стилі матриці.

Детальніше про функціонал:

- **Шифрування:** користувач вводить текст, натискає кнопку "Зашифрувати", текст шифрується за допомогою Fernet (симетричний алгоритм), ключ шифрування генерується випадково для кожного шифрування. Результат шифрування відображається у відповідному полі.
- **Дешифрування:** користувач вводить зашифрований текст, натискає кнопку "Розшифрувати", текст розшифровується за допомогою того ж ключа, що був використаний для шифрування. Результат дешифрування відображається у відповідному полі.
- **Генерація паролів:** користувач вказує бажану довжину пароля, натискає кнопку "Згенерувати пароль", генерується випадковий пароль заданої

довжини, що складається з літер, цифр та символів пунктуації. Згенерований пароль відображається на екрані та автоматично копіюється в буфер обміну.

- **Історія:** в окремій вкладці відображається історія всіх операцій шифрування та дешифрування.

Переваги коду:

- **Безпека:** використання Fernet забезпечує надійне шифрування даних.
- **Зручність:** інтуїтивно зрозумілий інтерфейс робить використання додатку простим та зручним.
- **Функціональність:** додаток об'єднує в собі всі необхідні функції для роботи з криптографією.
- **Візуальна привабливість:** анімований фон додає додатку оригінальності.

Покращення:

- **Зберігання ключа шифрування:** на даний момент ключ шифрування генерується кожного разу заново. Було б корисно додати можливість зберігання ключа для повторного використання.
- **Використання асиметричного шифрування:** для більш безпечного обміну зашифрованою інформацією можна додати підтримку асиметричного шифрування (наприклад, RSA).
- **Розширені налаштування генерації паролів:** можна додати можливість вибору набору символів для генерації пароля (тільки літери, тільки цифри, тощо).
-

Детальний опис коду

Код являє собою застосунок для шифрування, дешифрування та генерації паролів з графічним інтерфейсом, розроблений на Python з використанням бібліотек Tkinter, ttk, cryptography та інших.

Структура коду:

1. Імпорти:

- *tkinter* та *ttk*: для створення графічного інтерфейсу.

- *messagebox* та *filedialog*: для відображення повідомлень та діалогових вікон.
- *Fernet* з *cryptography*: для симетричного шифрування та дешифрування.
- *secrets*: для генерації криптографічно стійких випадкових чисел.
- *random*: для генерації псевдовипадкових чисел (використовується в анімації фону).
- *threading*: для створення окремого потоку для анімації фону.
- *pyperclip*: для копіювання згенерованого пароля в буфер обміну.
- *string*: для роботи з рядками (використовується в генерації паролів).
- *time*: для керування часом (використовується в анімації фону).

2. Клас *AdvancedMatrixBackground*:

- Створює анімований фон у стилі матриці з динамічними символами та кольорами.
- Використовує окремий потік для анімації, що забезпечує плавність та не блокує основний потік програми.

3. Клас *UltraSecureEncryptionApp*:

- Головний клас застосунку, що відповідає за створення та керування інтерфейсом.
- Містить методи для налаштування вкладок, обробки подій та виконання криптографічних операцій.

4. Методи класу *UltraSecureEncryptionApp*:

- *setup_main_container()*: створює головний контейнер та розміщує в ньому інші елементи інтерфейсу.
- *setup_styles()*: налаштовує стилі для віджетів для покращення читабельності.
- *create_notebook()*: створює вкладки для різних функцій застосунку (шифрування, дешифрування, генерація паролів, історія).
- *setup_encrypt_tab()*: налаштовує вкладку для шифрування тексту.

- *encrypt_text_function()*: функція для шифрування тексту за допомогою Fernet.
- *setup_decrypt_tab()*: налаштовує вкладку для дешифрування тексту.
- *decrypt_text_function()*: функція для дешифрування тексту за допомогою Fernet.
- *setup_password_tab()*: налаштовує вкладку для генерації паролів.
- *generate_password()*: функція для генерації пароля заданої довжини.
- *setup_history_tab()*: налаштовує вкладку для відображення історії операцій.
- *update_history_display()*: оновлює відображення історії шифрування та дешифрування.

5. Основний запуск програми:

- Створюється головне вікно Tkinter та екземпляр класу UltraSecureEncryptionApp.
- Запускається основний цикл обробки подій Tkinter (*root.mainloop()*).

Висловлення щодо коду

Код демонструє хороший рівень організації та використання сучасних практик програмування на Python. Особливо варто відзначити наступні моменти:

- **Потокобезпечність:** використання окремого потоку для анімації фону запобігає зависанню інтерфейсу під час виконання анімації.
- **Безпека:** використання Fernet забезпечує надійне шифрування даних.
- **Зручність:** інтуїтивно зрозумілий інтерфейс робить використання застосунку простим та зручним.
- **Функціональність:** застосунок об'єднує в собі всі необхідні функції для роботи з криптографією.
- **Візуальна привабливість:** анімований фон додає застосунку оригінальності.

Рекомендації щодо покращення:

- **Зберігання ключа шифрування:** на даний момент ключ шифрування генерується кожного разу заново, що не дуже зручно. Було б корисно додати можливість зберігання ключа для повторного використання.
- **Використання асиметричного шифрування:** для більш безпечного обміну зашифрованою інформацією можна додати підтримку асиметричного шифрування (наприклад, RSA).
- **Розширені налаштування генерації паролів:** можна додати можливість вибору набору символів для генерації пароля (тільки літери, тільки цифри, тощо).
- **Покращення інтерфейсу:** можна додати більше візуальних елементів, таких як іконки, для покращення сприйняття інтерфейсу користувачем.