Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки імені
професора Володимира Бурячка

«Допущено до захисту»
Завідувач кафедри інформаційної
та кібернетичної безпеки імені
професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття другого (магістерського)
рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ТРАФІКУ МЕСЕНДЖЕРІВ НА МОБІЛЬНИХ ПРИСТРОЯХ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ З БЕЗПЕКИ

Виконав

студент групи БІКСм-1-24-1.4д

Дем'янчук Андрій Сергійович
(прізвище, ім'я, по батькові)

_____
(підпис)

Науковий керівник

Д.т.н., професор
(науковий ступінь, наукове звання)

ГУЛАК Г.М.
(прізвище, ініціали)

_____
(підпис)

Київ – 2025

Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Освітньо-кваліфікаційних рівень – магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітня програма 125.00.01 Безпека інформаційних і комунікаційних систем

«Затверджую»
Завідувач кафедри
інформаційної та кібернетичної
безпеки імені професора
Володимира Бурячка кандидат
технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Дем'янчуку Андрію Сергійовичу

1. Тема роботи: Дослідження методів захисту трафіку месенджерів на мобільних пристроях та вироблення рекомендацій з безпеки;
2. Керівник д.т.н., професор ГУЛАК Г.М.

   затверджені наказом ректора від «___»____ 20___ року №__.
3. Термін подання студентом роботи «12» грудня 2025 р.
4. Вихідні дані до роботи:
   - 4.1 Теоретичні дані про вимоги законодавства України та документів щодо забезпечення безпеки кіберпростору
   - 4.2 Теоретичні дані про методи захисту трафіку месенджерів на мобільних пристроях
   - 4.3 Огляд популярних месенджерів в світі та в Україні
   - 4.4 Стандарт OWASP MOBILE APPLICATION SECURITY
   - 4.5 Результати дослідження
5. Зміст текстової частини роботи (перелік питань, які потрібно розробити):
   - 5.1 Вимоги законодавства України щодо забезпечення безпеки кіберпростору.
   - 5.2 Аналітичний огляд поточного стану забезпечення безпеки месенджерів.
   - 5.3 Формування вимог до проєктування механізмів забезпечення безпеки месенджерів згідно стандарту OWASP MOBILE APPLICATION SECURITY .
6. Перелік графічного матеріалу:
   - 6.1 Презентація доповіді, виконана в Microsoft PowerPoint.
7. Дата видачі завдання «___»_____ 20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання	02.06.2025	
2.	Пошук літератури	03.06.2025 - 30.06.2025	
3.	Обґрунтування вибору рішення	01.07.2025	
4.	Збір даних	02.07.2025 – 31.07.2025	
5.	Виконання та оформлення розділу 1.	01.08.2025 – 29.08.2025	
6.	Виконання та оформлення розділу 2.	01.09.2025 – 30.09.2025	
7.	Виконання та оформлення розділу 3.	01.10.2025 – 31.10.2025	
8.	Вступ, висновки, реферат	03.11.2025 – 19.11.2025	
9.	Апробація роботи на науково-методичному семінарі та/або науково-технічній конференції	15.05.2025, 26.10.2025	
10.	Оформлення та друк текстової частини роботи	20.11.2025 – 04.12.2025	
11.	Оформлення презентацій	05.12.2025 – 09.12.2025	
12.	Отримання рецензій	10.12.2025	
13.	Попередній захист роботи		
14.	Захист в ЕК		

Студент _____ Дем’янчук Андрій Сергійович
(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ Гулак Геннадій Миколайович
(підпис) (прізвище, ім’я, по батькові)

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженням методів захисту трафіку месенджерів на мобільних пристроях та вироблення рекомендацій з безпеки.

Робота складається зі вступу, трьох розділів, що містять 14 рисунків, 3 таблиці, висновків та списку використаних джерел, що містить 45 найменування. Загальний обсяг роботи становить 113 сторінок, перелік умовних скорочень та список використаних джерел.

Об'єктом дослідження в роботі є процеси забезпечення безпеки застосування месенджерів на мобільних пристроях.

Предметом дослідження є інструменти, політика конфіденційності та захищеності месенджерів.

Метою роботи є дослідження методів захисту месенджерів на мобільних пристроях, аналіз вірогідних загроз та вразливостей, що можуть негативно вплинути на стан захищеність месенджерів.

Для досягнення поставленої мети у роботі:

проведено аналіз існуючих сучасних месенджерів, їх методи захисту трафіку, їх функції забезпечення конфіденційності даних;

досліджено особливості функції безпеки месенджерів Google Messages, Facebook Messenger, WhatsApp, Viber, Telegram, Signal, Threema;

обґрунтовано, що надійна та ефективна безпека месенджерів досягається за рахунок комплексного підходу, який поєднує технічні засоби, тренінги і навчання користувачів.

Наукова новизна одержаних результатів полягає в тому, що в роботі на основі системного підходу до управління безпекою сучасних месенджерів на таких відповідальних етапах їх життєвого циклу, як проєктування та використання вперше запропоновані методичні рекомендації щодо впровадження організаційно-технічних заходів з блокування або нейтралізації загроз витоку конфіденційної інформації.

Галузь застосування. Запропоновані підходи можуть бути використані для підвищення ефективності функцій захисту в нових месенджерах або в модернізації вже існуючих месенджерів.

МЕСЕНДЖЕРИ, БЕЗПЕКА МЕСЕНДЖЕРІВ, ДВОХФАКТОРНА АВТЕНТИФІКАЦІЯ, НАСКРІЗНЕ ШИФРУВАННЯ, АНАЛІЗ ФУНКЦІЙ БЕЗПЕКИ, ПОРІВНЯННЯ МЕСЕНДЖЕРІВ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

2FA – двохфакторна аутентифікація

AES-256 (Advanced Encryption Standard 256) – симетричний алгоритм блочного шифрування

Bcrypt — адаптивна криптографічна функція формування ключа

CERT-UA – національна команда реагування на кіберінциденти, кібератаки, кіберзагрози

CSIRT - галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози

CSIRT-NBU - галузевий CSIRT, що діє у складі національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози

Double Ratchet – алгоритм шифрування, що використовується для забезпечення безпечного обміну повідомленнями між двома користувачами

E2EE (end-to-end encryption) – наскрізне шифрування

GDPR – загальний регламент про захист даних (General Data Protection Regulation)

HIPAA – федеральний закон США про мобільність та підзвітність медичного страхування

IDS - система виявлення вторгнень

IPS - система запобігання вторгненням

ISO/IEC 27001 – міжнародний стандарт, який визначає вимоги до Системи Управління Інформаційною Безпекою (СУІБ)

MIL.CERT-UA - галузевий CSIRT, що діє у складі Центру кіберзахисту Міністерства оборони України

MITM (man-in-the-middle) – кібератака

MFA – багатофакторна аутентифікація

NIST SP 800-63 – серія рекомендацій від Національного інституту стандартів і технологій (NIST) США

NIS 2 Directive – оновлена Директива Європейського Союзу

OAuth - протокол авторизації

PCI DSS – стандарт безпеки даних, прийнятий в індустрії платіжних карток.

SSL – криптографічний протокол, який забезпечує безпечне з'єднання між клієнтом і сервером в Інтернеті

Scrypt – криптографічний алгоритм

SDK (Software Development Kit) — це пакет інструментів, документації, прикладів коду та бібліотек

SCA (Software Composition Analysis) – автоматизований процес аналізу програмного забезпечення

TLS 1.3 – остання версія протоколу Transport Layer Security (TLS)

ЗМВР - захищений месенджер вітчизняної розробки

Обфускація коду – процес перетворення програмного коду на нечитабельну, заплутану версію

Реверс-інжиніринг — процес аналізу готового виробу, програми чи системи з метою зрозуміти їхню структуру

Тампериг (від англ. tampering) — незаконне втручання, підробка або фальсифікація чогось

Форс-браузинг – техніка атаки

ШІ - штучний інтелект

ВСТУП

В наш час використання месенджерів є одним з найважливіших способів комунікації між друзями, родиною, колегами. Вони дозволяють підтримувати зв’язок в будь якій точці світу, дають можливість обмінюватись фотографіями, аудіо, відео та іншими файлами.

На поточний час вже є достатня кількість різноманітних месенджерів, які відрізняються своїм функціоналом, захищеністю та доступністю.

Вибір месенджера загалом залежить від культурних та технічних уподобань, тому розробник робить все для того аби зробити інтерфейс месенджера простим та зручним, але з великим функціоналом.

Поверхнево більшість месенджерів вже зроблені зручними, мають функції використання біометричних даних, мають можливість збереження в хмарі приватних фото, відео для відновлення, мають функції відслідковування користувача. Тому з’являються питання, а як бути з серединою месенджера, чи є він безпечним для користування, чи є ймовірність що приватні данні користувачів не будуть перехоплені та продані або просто злиті в інтернет для шантажу або спаму?

Для формування всіх аспектів загроз користування месенджерами потрібно проаналізувати структуру месенджерів, поширені атаки на месенджери, сценарії атак, дослідити порушення, які допускав розробник, отримуючи персональні данні користувачів.

Для розробки рекомендацій методів захисту трафіку месенджерів необхідно дослідити вище зазначені фактори, розглянути ефективні способи протистояння загрозам, виділити загальні вразливості месенджерів.

Актуальність роботи полягає в тому, що месенджерів стає все більше, це є важлива частинна спілкування людей один з одним, тому існує ймовірність втрати персональних даних без дозволу користувача через недбалість засновника або вразливості в застосунку що призведе до можливого шантажу або інших

негативних наслідків.

Метою роботи є дослідження методів захисту месенджерів на мобільних пристроях, аналіз вірогідних загроз та вразливостей, що можуть негативно вплинути на стан захищеність месенджерів.

Завдання роботи сфокусовано на аналіз існуючих месенджерів, на пошук вразливостей в месенджерах, та дослідження методів перехоплення трафіку.

Об’єктом дослідження в роботі є процеси забезпечення безпеки застосування месенджерів на мобільних пристроях.

Предметом дослідження є методи та інструменти реалізації політики безпеки месенджерів.

Методи дослідження в роботі: проведено аналіз існуючих сучасних месенджерів, їх методи захисту трафіку, їх функції забезпечення конфіденційності даних;

досліджено особливості функцій безпеки месенджерів Google Messages, Facebook Messenger, WhatsApp, Viber, Telegram, Signal, Threema;

обґрунтовано, що надійна та ефективна безпека месенджерів досягається за рахунок комплексного підходу, який поєднує технічні засоби, тренінги і навчання користувачів.

Наукова новизна отриманих результатів полягає в тому, що в роботі на основі системного підходу до управління безпекою сучасних месенджерів на таких відповідальних етапах їх життєвого циклу, як проєктування та використання вперше запропоновані методичні рекомендації щодо впровадження організаційно-технічних заходів з блокування або нейтралізації загроз витоку конфіденційної інформації.

Проведене дослідження дозволяє стверджувати, що сучасні месенджери залишаються джерелом значних ризиків для конфіденційності та інформаційної безпеки. Найбільш критичними є витоки даних через програмні вразливості, збирання та аналіз метаданих, неконтрольоване використання чат-ботів та

інтеграції зі сторонніми сервісами, а також соціальні ризики поширення дезінформації.

Для України актуальним є впровадження національних стандартів безпеки разом з GDPR, забезпечення наскрізного шифрування за замовчуванням, підвищення рівня цифрової грамотності користувачів та посилення відповідальності компаній і адміністраторів за прозорість обробки даних та розповсюдження дезінформації

Майбутні дослідження варто спрямувати на вивчення каналів витоку метаданих, удосконалення механізмів аудиту політик конфіденційності та оцінку ефективності правових змін у сфері кібербезпеки.

Практичне значення одержаних результатів серед яких, нові методи рекомендацій у ході роботи можуть бути застосовані в нових месенджерах або в модернізації вже існуючих месенджерів.

Галузь застосування. Запропоновані підходи можуть бути використані для підвищення ефективності функцій захисту в нових месенджерах або в модернізації вже існуючих месенджерів.

Апробація результатів дипломної роботи. Основні положення роботи викладалися:

1) в тезах доповіді на XII Всеукраїнській науково-практичній конференції молодих учених «Інформаційні технології - 2025» (Київ: Київський університет імені Бориса Грінченка, 15 травня 2025 року) [41];

2) в тезах доповіді на студентській науковій конференції «Безпека інформаційно-комунікаційних систем (БІКС’2025)» (Київ: Київський університет імені Бориса Грінченка, 26 жовтня 2025 року) [42].

РОЗДІЛ 1

ВИМОГИ ЗАКОНОДАВСТВА УКРАЇНИ ТА НОРМАТИВНІ ДОКУМЕНТИ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІБЕРПРОСТОРУ

1.1. Система забезпечення кібербезпеки держави

Формування та реалізація державної політики у сфері кібербезпеки, захист прав і свобод людини та громадянина, національних інтересів України у кіберпросторі, боротьба з кіберзлочинністю забезпечується Кабінетом Міністрів (КМ) України. Уряд України також 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). КМ України є вищим органом у системі органів виконавчої влади, який реалізує свої функції безпосередньо та через міністерства, інші центральні органи виконавчої влади [1].

1.1.1 Перелік і засади розмежування компетенції суб’єктів забезпечення кібербезпеки в Україні

Загальний перелік і засади розмежування компетенції суб’єктів забезпечення кібербезпеки визначаються у ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України». Зокрема, зазначеною статтею передбачено, що координація діяльності у сфері кібербезпеки здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони (РНБО) України. Робочим органом РНБО України у вказаній сфері є національний координаційний центр кібербезпеки, який здійснює координацію та контроль за діяльністю суб’єктів сектору безпеки і оборони, котрі забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування й уточнення Стратегії кібербезпеки України [1][2].

У ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» прописано, що національна система кібербезпеки є сукупністю суб’єктів

забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури [2].

Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи України, Національний банк України, Міністерство закордонних справ України, які відповідно до Конституції і законів України виконують у встановленому порядку такі основні завдання.

Державна служба спеціального зв’язку та захисту інформації України забезпечує формування та реалізацію державної політики з кіберзахисту державних інформаційних ресурсів та інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, активної протидії агресії в кіберпросторі, кіберзахисту критичної інфраструктури, здійснює державний контроль у зазначених сферах; здійснює стандартизацію у сферах криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам; забезпечує створення та функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, координує діяльність інших суб’єктів забезпечення кібербезпеки щодо кіберзахисту, забезпечує створення та функціонування Національної електронної комунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA (національний CSIRT), систематично організовує та проводить навчання з питань технічного захисту та кіберзахисту

для осіб, які в межах своєї компетенції безпосередньо здійснюють заходи з кіберзахисту в органах державної влади, органах місцевого самоврядування, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, та в юридичних особах, які є власниками або розпорядниками об'єктів критичної інфраструктури або об'єктів критичної інформаційної інфраструктури, забезпечує функціонування системи професійної кваліфікації за групами кваліфікацій у сферах захисту інформації та кіберзахисту, здійснює методичне регулювання оцінювання стану кіберзахисту, встановлює вимоги до суб'єктів оцінювання стану кіберзахисту щодо оцінювання інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури; виконує інші завдання та здійснює інші повноваження відповідно до закону [2].

Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, кримінальних правопорушень проти об'єктів критичної інформаційної інфраструктури, здійснює заходи з інформування громадян про безпеку в кіберпросторі [2].

Служба безпеки України відповідно до закону здійснює заходи із запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти основ національної безпеки України, миру і безпеки людства, а також кримінальних правопорушень терористичної спрямованості, що вчиняються у кіберпросторі або з його використанням, здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом, кібердиверсіями та кібершпигунством; координує діяльність суб'єктів забезпечення кібербезпеки щодо протидії кібершпигунству, кібертероризму,

кібердиверсіям, негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти, кібератаки та кіберзагрози у сфері державної безпеки [2].

Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони), здійснюють військову співпрацю з НАТО, міжнародними організаціями та іншими суб’єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз.

Розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює Центр кіберзахисту Національного банку України (включаючи команду реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT-NBU), забезпечує функціонування системи кіберзахисту для банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; забезпечує функціонування системи оцінювання стану кіберзахисту в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг,

державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг; встановлює вимоги до проведення аудиту інформаційної безпеки в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг [2].

Міністерство закордонних справ України сприяє розвитку євроінтеграційних процесів щодо підходів, методів, засобів забезпечення кібербезпеки, здійсненню узгоджених із ключовими міжнародними партнерами заходів, спрямованих на посилення кіберстійкості України та розвиток спроможностей національної системи кібербезпеки; забезпечує координацію діяльності щодо співпраці з міжнародними партнерами для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці; забезпечує активну участь України в діяльності міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної міжнародної нормативно-правової бази; сприяє проведенню спільних з Європейським Союзом заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати і переслідувати кіберзлочинність та реагувати на кіберзагрози; координує процес запровадження гармонізованого з євроатлантичною спільнотою підходу до застосування санкцій у відповідь на підривну діяльність у кіберпросторі, узгодження з міжнародними партнерами механізму спільних дипломатичних дій і заходів у відповідь на деструктивну кіберактивність; виконує інші завдання відповідно до закону [2].

Виходячи з вище зазначеного, 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 та контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності, Збройні Сили (ЗС) України, інші військові формування, утворені відповідно до закону, Національний банк

України, підприємства, установи й організації, віднесені до об'єктів критичної інфраструктури, суб'єкти господарювання, громадяни України й 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 [1]. Ролі агенцій з кібербезпеки зазначені в таблиці 1.1 [3, с.35].

Таблиця 1.1

Ролі агенцій з кібербезпеки

Міжнародне співробітництво	Кіберінциденти / кібератаки/ кіберзагрози	Захист об'єктів КІ	Кіберзлочини	Державна політика/ інформування громадськості
Взаємо-допомога (Генеральна прокуратура (досудовий етап), Міністерство юстиції (етап суду), Міністерство закордонних справ (за відсутності угоди)	ДССЗЗІ (усі кіберінциденти/ атаки, CERT-UA, інформування про кіберзагрози)	СБУ (контррозвідувальна та оперативно-розшукова діяльність, перевірка готовності до кіберінцидентів і кібератак)	СБУ (злочини проти миру і безпеки людства, злочини, що можуть вплинути на життєві інтереси України, кібертероризм і кібершпіонаж)	ДССЗЗІ (політика у сфері захисту державних інформаційних ресурсів)
Точка контакту 24/7 (Міністерство юстиції (у справах судів), Генеральна прокуратура (органи досудового розслідування), Міністерство внутрішніх справ)	СБУ (об'єкти КІ, державна безпека, державні електронні ресурси, критична інформаційна інфраструктура, Ситуаційний центр забезпечення кібербезпеки)	ДССЗЗІ (кібер-захист, аудит об'єктів КІ, впровадження незалежного аудиту інформаційної безпеки)	Національна поліція (запобігання, виявлення, припинення і розслідування)	Національна поліція (інформування громадськості про кібербезпеку)
Міністерство оборони (військове співробітниц-тво з НАТО)	Розвідувальні органи (розвідувальна діяльність щодо кіберзагроз)	Міністерство оборони (у випадку надзвичайного або воєнного стану)		

У межах своєї компетенції суб'єкти забезпечення кібербезпеки здійснюють: заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-

підривних, терористичних та інших протиправних і злочинних цілях; виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; інформаційний обмін щодо реалізованих і потенційних кіберзагроз, розробку і реалізацію запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту, проведення аудиту інформаційної безпеки, у т. ч. на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління, інші заходи із забезпечення розвитку та безпеки кіберпростору [1].

Законодавче підґрунтя забезпечення кібербезпеки, відповідно до якого визначається компетенція суб'єктів її забезпечення, становлять Конституція України, Стратегія національної безпеки України, Стратегія кібербезпеки України, Доктрина інформаційної безпеки України, Закони України «Про національну безпеку України», «Про Раду національної безпеки і оборони України», «Про Службу безпеки України», «Про Державну Службу спеціального зв'язку і захисту інформації України», Положення про Національний координаційний центр кібербезпеки тощо [1].

У 2017 р. Президент України підписав Указ «Про Національний координаційний центр кібербезпеки», яким затверджено Положення про вказаний центр. До його основних завдань належить аналіз стану кібербезпеки, результатів проведення огляду національної системи кібербезпеки, стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури, даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо. Відповідно до Указу Президента України № 27/2020 штат апарату РНБО розширено до 190 співробітників для забезпечення інформаційно-аналітичного, експертного, організаційного, матеріально технічного забезпечення Центру, розширено повноваження Центру, який

координує та контролює роботу суб'єктів сектору безпеки і оборони у сфері кібербезпеки [1].

Втім, слід зауважити, що відповідні законодавчі новації, особливо у контексті змісту внесеного Президентом України законопроекту № 3196 зумовлюють ризик взаємного дублювання повноважень Центру кібербезпеки, СБ України та ДСС України. Тож відповідна проблема підлягає врегулюванню в ході подальшого вдосконалення системи суб'єктів забезпечення кібербезпеки. Так само потребують вдосконалення та розвитку питання державно-приватного партнерства у сфері кібербезпеки [1][4].

1.2 Організаційно-технічні аспекти забезпечення безпеки кіберпростору

Забезпечення кіберпростору – це комплексний процес, як технічно так і організаційно. В 9 статті закону України «Про основні засади забезпечення кібербезпеки України» прописано наступне.

В Україні створюється та забезпечується функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури.

Уповноваженим органом, що забезпечує функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, є Державна служба спеціального зв'язку та захисту інформації України [2].

До складу національної системи реагування на кіберінциденти, кібератаки, кіберзагрози входять:

1. CERT-UA – національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (національний CSIRT), діяльність якої забезпечується Державною службою спеціального зв'язку та захисту інформації України.

2. Галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (далі - галузеві, регіональні CSIRT) – створюються органами державної влади або органами місцевого самоврядування з метою посилення спроможності національної системи реагування на кіберінциденти, кібератаки, кіберзагрози у відповідній галузі, сфері або відповідному регіоні з урахуванням вимог до організаційно-технічної спроможності, встановлених Державною службою спеціального зв'язку та захисту інформації України, та взаємодіють з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності, іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози в порядку, встановленому Кабінетом Міністрів України.

3. Національна поліція України, Служба безпеки України – взаємодіють у рамках національної системи реагування на кіберінциденти, кібератаки, кіберзагрози з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози в порядку, встановленому Кабінетом Міністрів України, з урахуванням вимог цього Закону та в межах повноважень, визначених законом.

4. Приватні команди реагування – можуть залучатися для надання операторам критичної інфраструктури, власникам або розпорядникам критичної інформаційної інфраструктури, органам державної влади та органам місцевого самоврядування окремих послуг, пов'язаних з реагуванням на кіберінциденти, виконання окремих завдань галузевих, регіональних CSIRT, а також взаємодіяти з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, у тому числі щодо обміну інформацією.

5. Національний координаційний центр кібербезпеки – здійснює загальну координацію функціонування суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози [2].

1.2.1 CERT-UA

Завданнями CERT-UA (національний CSIRT) є:

- Моніторинг, накопичення та проведення аналізу даних про кіберінциденти, кібератаки, кіберзагрози на національному, галузевому, регіональному рівнях, динамічний аналіз ризиків та ситуаційної обізнаності.
- Отримання та опрацювання у встановленому порядку обов'язкових та інших повідомлень про кіберінциденти, здійснених у межах функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози відповідно до цього Закону, надання рекомендацій щодо можливих заходів реагування та технічної підтримки.
- Здійснення у встановленому порядку заходів щодо надання попереджень про кіберзагрози, сповіщень, оголошень та інформування щодо кіберінцидентів, кібератак, кіберзагроз та вразливостей органів державної влади, державних органів, органів місцевого самоврядування, операторів критичної інфраструктури, власників та розпорядників критичної інформаційної інфраструктури у режимі, за можливості, наближеному до реального часу.
- Надання у встановленому порядку сервісу у зв'язку з реагуванням, рекомендацій з реагування на кіберінциденти, кібератаки, кіберзагрози власникам або розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, операторам критичної інфраструктури, власникам або розпорядникам критичної інформаційної інфраструктури, іншим суб'єктам.
- Виконання функції координатора з метою узгодженого розкриття вразливостей.
- Інформування у встановленому законодавством порядку Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України про кіберінциденти, кібератаки, кіберзагрози, виявлені або потенційні вразливості інформаційних, електронних комунікаційних та інформаційно-комунікаційних

систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також об'єктів критичної інформаційної інфраструктури із зазначенням обов'язкових та/або рекомендованих заходів реагування для видання вимоги про реагування [2].

- Проведення аналізу ризиків у зв'язку з кіберінцидентом, кібератакою, кіберзагрозою та надання відповідних рекомендацій.
- Забезпечення у встановленому порядку функціонування репозитарію інформації про кіберінциденти, таксономій кіберінцидентів та їх версій.
- Взаємодія у встановленому порядку з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози.
- Взаємодія у встановленому порядку із суб'єктами національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози.
- Взаємодія у встановленому порядку з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності в межах, необхідних для виконання ними повноважень, визначених законом.
- Виконання функцій національного контактного центру відповідно до Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS 2 Directive).
- Взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, кібератаки, кіберзагрози, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків.

1.2.2 Галузеві та регіональні CSIRT

Альтернативою створення органами державної влади або органами місцевого самоврядування власних галузевих, регіональних CSIRT є залучення послуг приватних команд реагування, що можуть виконувати у повному обсязі або частково завдання галузевого, регіонального CSIRT відповідно до цього Закону та за умови дотримання ними встановлених законодавством вимог до таких галузевих, регіональних CSIRT [2].

Галузевим, регіональним CSIRT у порядку, визначеному Державною службою спеціального зв'язку та захисту інформації України, делегуються від національного CSIRT завдання щодо:

- Моніторингу та проведення аналізу даних про інциденти кібербезпеки, кібератаки, кіберзагрози у відповідній галузі або відповідному регіоні, динамічного аналізу ризиків та ситуаційної обізнаності.
- Отримання та опрацювання у встановленому порядку обов'язкових та інших повідомлень про кіберінциденти у відповідній галузі або відповідному регіоні, отриманих у межах функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози згідно з цим Законом [2], надання рекомендацій щодо можливих заходів реагування та технічної підтримки.
- Здійснення у встановленому порядку заходів щодо надання попереджень про кіберзагрози, сповіщень, оголошень та інформування щодо кіберінцидентів, кібератак, кіберзагроз та вразливостей у відповідній галузі або відповідному регіоні у режимі, за можливості, наближеному до реального часу.
- Надання у встановленому порядку сервісу у зв'язку з реагуванням, рекомендацій з реагування на кіберінциденти, кібератаки, кіберзагрози у відповідній галузі або відповідному регіоні.

Державна служба спеціального зв'язку та захисту інформації України має право надавати вимоги про усунення порушень у діяльності галузевого, регіонального CSIRT у разі невідповідності вимогам щодо організаційно-технічної спроможності або порушення порядку функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози або національної системи реагування на кіберінциденти, кібератаки, кіберзагрози.

Команда реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT-NBU, що входить до складу Центру кіберзахисту Національного банку України, є галузевим CSIRT та діє у складі національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та національної системи реагування на

кіберінциденти, кібератаки, кіберзагрози з урахуванням постанов Національного банку України в частині, що не суперечить цьому Закону [2].

Центр кіберзахисту Міністерства оборони України (MIL.CERT-UA) є галузевим CSIRT та діє у складі національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та національної системи реагування на кіберінциденти, кібератаки, кіберзагрози з урахуванням організаційно-розпорядчих актів Міністерства оборони України в частині, що не суперечить цьому Закону.

Служба безпеки України забезпечує функціонування Ситуаційного центру забезпечення кібербезпеки Служби безпеки України та регіональних центрів забезпечення кібербезпеки регіональних органів Служби безпеки України для виконання завдань щодо протидії шпигунству, тероризму, диверсіям та в межах повноважень, визначених законом, протидії іншим кіберзагрозам у сфері державної безпеки.

1.2.3 Координація функціонування суб'єктів національної системи реагування на кіберінциденти, кібератаки та кіберзагрози

Державна служба спеціального зв'язку та захисту інформації України та Служба безпеки України з метою вжиття заходів оперативного реагування на кіберінциденти, кібератаки, кіберзагрози в межах своїх повноважень можуть надавати обов'язкові до виконання вимоги про реагування власникам або розпорядникам інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури, операторам критичної інфраструктури.

Таке оперативне реагування шляхом надання вимоги про реагування на кіберінциденти, кібератаки, кіберзагрози є актом організаційно-розпорядчого характеру, не є заходом державного контролю за технічним захистом інформації та кіберзахистом та здійснюється з метою запобігання або мінімізації негативних наслідків у зв'язку з кіберінцидентом, кібератакою або кіберзагрозою [2].

Власники або розпорядники інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, оператори критичної інфраструктури, власники або розпорядники об’єктів критичної інформаційної інфраструктури зобов’язані вжити визначених вимогою про реагування на кіберінциденти, кібератаки, кіберзагрози заходів та подати звіт про результати вжитих заходів у строки та порядку, встановлені Державною службою спеціального зв’язку та захисту інформації України [2].

Підстави для надання вимоги про реагування на кіберінциденти, кібератаки, кіберзагрози, строки та порядок подання звіту про результати вжитих заходів встановлюються Державною службою спеціального зв’язку та захисту інформації України.

Суб’єкти національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, крім приватних компаній, що не здійснюють функцій галузевих, регіональних CSIRT, забезпечують у порядку, визначеному для функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, невідкладне інформування Національного координаційного центру кібербезпеки про всі значні кіберінциденти, кібератаки [2].

Для забезпечення скоординованого, оперативного та ефективного реагування на кризову ситуацію у зв’язку з кіберінцидентом, кібератакою, кіберзагрозою у складі Національного координаційного центру кібербезпеки утворюється та функціонує постійно діюча Об’єднана група реагування на кіберінциденти, кібератаки, кіберзагрози, до складу якої входять представники Національного координаційного центру кібербезпеки, Державної служби спеціального зв’язку та захисту інформації України, Служби безпеки України, Національної поліції України та представники інших основних суб’єктів національної системи кібербезпеки (за обґрунтованої необхідності) [2].

Щодо технічної частини то туди входять: антивірусне програмне забезпечення, системи виявлення вторгнень, шифрування даних, брандмауери та регулярне оновлення системи.

Розглянемо приклади антивірусного забезпечення:

ESET NOD 32 – платний антивірусний пакет від словацької фірми. Можна використовувати як для персонального пристрою так і для підприємств, державних установ та навіть для великих корпоративних мереж. Має великий функціонал для захисту від вірусів, троянів та шпигуньских програм до захисту від небезпечних веб ресурсів.

Bitdefender – румунський антивірус, який теж платний. Має функції захисту вебкамери, анти-фішинг, блокування вірусів та захист від шпигунства.

Avast – антивірусна програма від чехів. Підходить під операційні системи Windows, Linux, macOS, Android та iOS. Спеціалізується на захисті пошти, блокуванні зловмисних сайтів.

Приклади систем виявлень:

Snort – це провідна у світі система запобігання вторгненням (IPS) з відкритим кодом. Snort IPS використовує низку правил, які допомагають визначити шкідливу мережеву активність, і використовує ці правила для пошуку пакетів, що їм відповідають, та генерує сповіщення для користувачів [5].

Suricata – програма з відкритим вихідним кодом для попередження та виявлення мережевих вторгнень (IPS/IDS). Програма з відкритим вихідним кодом. Додатково є інструментом для аналізу пакетів.

Шифрування даних:

BitLocker – вбудована функція шифрування дисків в операційній системі Windows, допомагає захищати дані за рахунок повного або часткового шифрування диску. Допоможе у разі викрадення пристрою з метою викрадення даних.

NordLocker – сервіс для шифрування файлів та хмарного сховища, забезпечує захист для користувачів завдяки наскрізному шифруванню. Завдяки сервісу можна

безпечно зберігати файли на різних пристроях та створювати резервні копії файлів.

1.3 Сучасні технології кіберзахисту

Коли йдеться про зміцнення кіберзахисту і протистояння загрозам у кіберпросторі, важлива сукупність одразу кількох складових: досвідчені фахівці, сучасні технології та співпраця, зокрема з міжнародними партнерами [6].

Закривати очі на проблеми цифрового захисту сьогодні небезпечно як ніколи. За оцінками Cybersecurity Ventures кіберзлочинність у 2023 році глобально завдала понад $8 трлн збитків. Експерти прогнозують, що протягом наступних трьох років глобальні збитки від кіберзлочинності будуть зростати на 15% щороку. Якщо у 2015 році вони становили $3 трлн, то у 2025 році сягнуть позначки в $10,5 трлн. Для порівняння: це майже половина номінального ВВП США, який наразі становить близько $23 трлн.

Контролювати кіберзлочинність дуже важко. Експерти вважають, що глобально в поле зору правоохоронців потрапляють менш ніж 25% від усіх скоєних кіберзлочинів.

Ступінь ризиків суттєво виросла через стійкий тренд на віддалену працю та важке геополітичне середовище, де кібератаки стають важелем економічного і політичного впливу. Зокрема, близько третини від глобального потоку шкідливих email-розсилок беруть початок в РФ. Пов`язані з Росією угруповання також відповідальні за масовані ddos-атаки на інфраструктуру цивілізованих країн [7][8].

Сучасні технології кіберзахисту включають в себе машинне навчання та штучний інтелект для виявлення загроз, блокчейн для безпечного зберігання та передачі даних, а також виявлення та реагування на загрози на основі штучного інтелекту (AI XDR) для глибокого аналізу даних та автоматичного реагування на кібератаки.

Засоби ШІ розвиваються стрімко й неконтрольовано, і кіберзлочинці користуються цим. Вони вже навчилися створювати за допомогою генеративного

ШІ шкідливий код для автоматизованих malware-атак та застосовувати засоби генерації тексту, відео та зображень для фішингу й практик соціальної інженерії.

Та водночас експерти з кіберзахисту також опановують засоби ШІ – вони допомагають автоматично виявляти загрози в режимі реального часу, виявляти аномальну поведінку та фейковий згенерований контент, реалізовувати механізми смарт-аутентифікації й автоматичної відповіді на загрози [7].

В останні роки було проведено величезну роботу з розробки рішень на основі глибокого навчання для використання в додатках кібербезпеки, включаючи захист і оборону. Рішення на основі глибокого навчання здатні забезпечити чудову продуктивність, яка часто перевершує традиційне машинне навчання, що працює з великими наборами даних, і на даний момент є найсучаснішими в багатьох областях [9].

Однак вони мають деякі важливі обмеження, які слід враховувати під час розробки та впровадження. Перше з них – це доступність і надійність наборів даних, тобто необхідність великих наборів даних, що містять високоякісні дані. Переважна більшість літератури зосереджується на поліпшенні найсучаснішої продуктивності, тоді як надійність наборів даних майже не враховується [9].

У сучасній літературі пропонуються такі критерії надійності: різноманітність атак, анонімність, доступні протоколи, повне захоплення (з корисним навантаженням), повна взаємодія, повна конфігурація мережі, повний трафік, набір функцій, гетерогенність (весь мережевий трафік і системні журнали), правильне маркування та метадані (повна документація збору даних).

На жаль, існуючі критерії надійності зосереджуються на виявленні вторгнень, тоді як подібні вимоги для інших застосувань кібербезпеки ще не розглядалися.

Другим важливим аспектом, який слід враховувати в цьому конкретному контексті, є той факт, що зловмисники постійно розробляють нові типи атак, обходячи існуючі системи безпеки. Ця конкретна проблема належить до області

навчання в нестаціонарних середовищах і зазвичай називається концептуальним зсувом [9].

Крім того, система, що досліджується, може зазнати змін у своїх номінальних умовах експлуатації (часові зміни), що вимагає оновлення номінальної моделі. Такі зміни необхідно своєчасно виявляти та правильно ідентифікувати, щоб механізми захисту могли надійно функціонувати.

Тому навчання в нестаціонарних середовищах у сфері кібербезпеки залишається відкритим питанням, і для ефективних та сучасних моделей безпеки необхідні нові методи, здатні виявляти зміни стаціонарності та реагувати на них належним чином [9].

Інструменти та методології на основі ШІ можуть використовуватися для виявлення та ідентифікації кібератак і пом'якшення їх наслідків. Такі інструменти мають потенціал для забезпечення задовільної ефективності за низької вартості та в режимі реального часу. Існує широкий спектр технічних засобів захисту та можливостей, які можуть бути реалізовані за допомогою штучного інтелекту. Механізми захисту на основі штучного інтелекту все частіше застосовуються в галузі кібербезпеки, наприклад, для забезпечення безпеки мереж і даних, захисту кінцевих точок, надійності доступу тощо.

ШІ може використовуватися для оцінки вразливостей комп'ютерних систем та мереж. Алгоритми машинного навчання часто використовуються для аналізу даних з різних джерел, таких як сканери, журнали безпеки та системи управління виправленнями, з метою виявлення вразливостей та визначення пріоритетності заходів з їх усунення [9].

Більшість «традиційних» застосувань машинного навчання майже повністю належать до етапу виявлення, тобто виявлення спаму, вторгнень і шкідливого програмного забезпечення, а також виявлення атак. Велика кількість існуючих робіт зосереджена на виявленні спаму в комп'ютерних мережах. Спам в електронній пошті споживає відповідні ресурси (наприклад, пропускну здатність,

пам'ять тощо), безпосередньо зменшуючи потужність і ефективність систем та мереж.

У міру розвитку технологій ШІ в майбутньому ми, ймовірно, станемо свідками все більш витончених і складних кібератак, що базуються на ШІ. Наприклад, генеративна суперечлива мережа, клас фреймворків машинного навчання, вже використовуватися для створення «глибоких підробок» шляхом заміни або маніпулювання обличчями або голосами на зображенні або відео [9].

Алгоритми на основі ШІ також здатні готувати переконливі фішингові листи, спрямовані на окремих осіб та організації. ШІ також може використовуватися для підвищення ефективності та результативності шкідливого програмного забезпечення шляхом поліпшення його здатності уникати виявлення, адаптуватися до мінливих умов, націлюватися на конкретні вразливості, поширюватися та зберігатися в цільових системах. Шкідливе програмне забезпечення на основі ШІ може використовувати методи підкріплювального навчання для самовдосконалення та здійснення ще більш успішних атак.

Зловмисники можуть скористатися навчальними даними для створення «задніх дверей» в алгоритмі ШІ. Зловмисники також можуть використовувати ШІ для прийняття рішень щодо того, яку вразливість найімовірніше варто експлуатувати. Це лише кілька прикладів кібератак на основі ШІ, які вже викликають серйозне занепокоєння [9].

1.3.1 Блокчейн

Сьогодні про блокчейн передусім знають як про інструмент, що забезпечив нас криптовалютою та NFT. Однак потенціал технології виходить далеко за межі цифрових фінансових операцій. Те, що з’явилось як відповідь на світову кризу 2008 року, може стати тим самим рушієм, якого не вистачає багатьом сферам.

Блокчейн – це дистрибутивна база даних, яка забезпечує збереження й обмін інформацією без потреби в посередниках. Всі дані у вигляді «блоків» зберігаються на різних комп'ютерах (вузлах), що створює децентралізовану структуру. Кожен

блок містить запис про попередній, утворюючи ланцюг. Цей ланцюг неможливо змінити, що гарантує безпеку даних [10].

Основна перевага полягає в тому, що кожен блок містить криптографічний підпис, який підтверджує його достовірність. Коли нова інформація додається до блокчейну, її не можна змінити або видалити без внесення змін до всіх наступних блоків, що робить фальсифікацію майже неможливою.

Процес валідації нових транзакцій вимагає участі кількох учасників, і це дає змогу створювати систему, в якій довіра до інформації забезпечується не через централізовану організацію, а завдяки численним перевіркам різних учасників мережі [10].

Децентралізація, прозорість, незмінність і безпека робить блокчейн майже незамінною технологією для сучасних прогресивних індустрій, де на перше місце виходять швидкість, безпека даних та довіра між учасниками процесу. Саме тому сфери його використання набагато ширші, ніж фінансовий сектор.

Саме з фінансових операцій починається розквіт блокчейну, адже він значно підвищує ефективність і безпеку [9]. Так, JPMorgan запустив свою платформу, що дозволяє здійснювати миттєві транзакції між компаніями, знижуючи витрати й час на обробку. А в Goldman Sachs активно експериментують з приватними блокчейн-системами для скорочення часу на фінансові транзакції та підвищення прозорості. Крім того, блокчейн допомагає зменшити ризики шахрайства, що, погодьтеся, важливо, коли справа стосується фінансів. І хоча впровадження цієї технології досі відбувається повільно, саме тут очікують найбільшого прориву в наступні кілька років.

Ще одна зі сфер, яка потребує суттєвих змін і трансформацій це охорона здоров'я. Щодня вона стикається з багатьма викликами, серед яких – безпека даних, сумісність систем та операційна неефективність. Блокчейн пропонує рішення, зокрема в управлінні електронними медичними картами (EHR), де пацієнти зберігають контроль над своїми даними, а медичні працівники мають

безпечний доступ. Також блокчейн забезпечує прозорість клінічних випробувань і запобігає підробкам ліків завдяки відстеженню постачання. Блокчейн відкриває можливості для нових послуг, як-от децентралізоване медичне страхування та аналітика з використанням ШІ.

За допомогою блокчейну можна верифікувати дипломи та сертифікати, що знижує ризики підробок і спрощує перевірку даних. Освітні установи можуть зберігати важливі документи в незмінному форматі, а студенти — отримати контроль над своїми записами. Blockcerts використовує блокчейн для видачі цифрових сертифікатів, що робить процес верифікації простішим та безпечнішим.

Там, де є можливості, є і виклики. Від складнощів інтеграції з чинними системами до правових непорозумінь – кожен з цих бар'єрів може уповільнити розвиток блокчейну.

- Масштабування

Одна з найбільших проблем блокчейн-технології – здатність обробляти величезну кількість транзакцій. Щойно кількість користувачів або транзакцій зростає, пропускна здатність мережі знижується, що веде до затримок у виконанні операцій і підвищення їхньої вартості. У низці випадків це може обмежити практичне застосування технології до великих бізнесів чи глобальних платформ.

- Складність інтеграції

Для того, щоб інтегрувати блокчейн у вже наявні бізнес-системи, потрібно перепроєктувати інфраструктуру. Це може охоплювати зміну підходів до обробки даних, оновлення програмного забезпечення та навчання персоналу. Інтеграція з іншими технологіями або старими базами ускладнюється потребою узгоджувати різні системи й формати даних.

- Складність технології

Блокчейн – відносно нова технологія, яка вимагає знань про розподілені реєстри, шифрування і механізми консенсусу. Для розуміння блокчейну потрібно орієнтуватися, як він працює на рівні інфраструктури та як гарантується безпека

даних. Через це технологія може залишатися обмеженою і менш доступною для масового користування.

- Проблеми сумісності

Блокчейн-системи засновані на різних протоколах та стандартах, що перешкоджає їхній взаємодії між собою. Це означає, що платформи можуть мати труднощі в обміні даними або спільному використанні інформації, що, своєю чергою, сповільнює створення загальних стандартів та розширення застосування блокчейн-технологій на всіх рівнях.

- Високі витрати на впровадження

Перехід на блокчейн вимагає значних фінансових витрат. Це охоплює не тільки розробку та налаштування нових систем, але й навчання співробітників. Оскільки технологія потребує постійної підтримки, її експлуатація може бути надто дорогою, особливо для малих компаній.

Крім того, за всіх заяв про максимальну безпеку блокчейн гарантує вищий рівень захисту даних тільки в порівнянні з уже наявними рішеннями. Він менш вразливий до стандартних атак і краще протистоїть шахраям, які намагаються поцупити дані, але досі не дає 100% гарантій цілісності інформації [10].

1.3.2 Системи IDS та IPS

Варто не забувати вже і про існуючі технології які оновлюють свій захист наприклад:

Системи виявлення вторгнень (IDS) та запобігання вторгненням (IPS). IDS та IPS функціонують для досягнення спільної мети – захисту інфраструктури мережі. У більшості випадків ці системи виявляють дивну активність, порівнюючи її зі стандартними (нормальними) характеристиками поведінки. Обидві системи є хорошими варіантами для боротьби із загрозами, пов'язаними з мережевою інфраструктурою. Процес працює в основному шляхом аналізу активності трафіку і порівняння його з базою даних звичайної і аномальної активності. IDS

функціонує, аналізуючи активність трафіку, в той час як IPS може навіть впливати на цей процес і певним чином контролювати його [11].

IDS або система виявлення вторгнень зазвичай пов'язана з програмним забезпеченням або пристроєм, який відповідає за моніторинг онлайн-загроз, незалежно від того, чи знаходиться він в системі або мережі. Інформація про дивну активність зазвичай повідомляється адміністратору або збирається через систему SIEM. Варіанти виявлень різняться між собою, наприклад, виявлення аномалій. IDS може функціонувати для моніторингу комп'ютера, а також мережевої активності і після цього розділяти активність на нормальну або аномальну. Цей тип систем спочатку був розроблений для виявлення дивної активності. Підхід в основному заснований на використанні машинного навчання, за допомогою якого запам'ятовуються правильні моделі активності і порівнюються з новими/дивними. Цей підхід набагато кращий завдяки своїм узагальненим властивостям, але у вас можуть виникнути деякі проблеми з помилковими спрацьовуваннями. Виявлення IDS на основі підпису. Цей підхід вважається більш традиційним і базується на пошуку певних шаблонів. У цьому методі шаблони означають те ж саме, що і підписи. Таке виявлення IDS допоможе в боротьбі з відомими кібератаками, але матиме певні проблеми з новими шаблонами або ж виявлення на основі репутації. Тут оцінка репутації впливає на весь процес [11].

Основна класифікація включає два типи цієї системи:

- NIDS. Цей тип IDS контролює вхідний трафік. Ця система аналізує активність трафіку, який надходить на/з пристрою. Вся активність порівнюється з наявною бібліотекою можливих атак, і як тільки виявляється щось дивне, адміністратор отримує сповіщення про це.
- HIDS. Така система необхідна для належного моніторингу ОС на пристроях або окремих хостах. Усі пакети відстежуються з метою виявлення незвичайної активності. Сповіщення відбувається в разі зміни критичних файлів у системі.

IPS або система запобігання вторгненням функціонує шляхом виявлення загрозливої активності, повідомлення про таку активність і спроб запобігти таким

загрозам. Як правило, IPS знаходиться відразу за брандмауером. Цей тип систем надзвичайно корисний для виявлення проблем, пов'язаних зі стратегіями безпеки, виявлення кіберзлочинців та ідентифікації загроз документам [11].

Ось кілька методів, які пояснюють, як функціонує IPS:

- Моніторинг аналізу протоколів з урахуванням стану. Цей метод IPS функціонує шляхом порівняння всієї активності з узагальненими правилами, і таким чином виявляються відхилення.
- Моніторинг на основі підпису. Процес в методі IPS виявляє пакети в мережі, після чого стандартні шаблони (сигнатури) порівнюються з пакетами.
- Моніторинг на основі статистичних даних. Підхід функціонує шляхом перевірки мережевої активності, а порівняння проводиться на основі заздалегідь визначеної базової лінії. Ця лінія визначає основні характеристики, які вважаються нормальними, такі як використання певних протоколів або використовувана пропускна здатність. Якщо є певні проблеми з базовою конфігурацією, результат може бути хибнопозитивним.

Отже можна сказати що IPS потрібен для видалення загрозливого контенту або видалення заражених даних після кібератаки, для блокування користувача, який порушує певні шаблони, отримуючи доступ до мережі, хосту або програми [11].

Класифікація типів IPS:

WIPS. Цей тип IPS виявляє несанкціонований доступ і усуває його, як тільки помітив. Зазвичай така система функціонує як надбудова над інфраструктурою бездротової локальної мережі, але може використовуватися і самостійно. Завдяки використанню WIPS можна запобігти таким ризикам, як honeypot, несанкціоновані точки доступу, атаки на відмову в обслуговуванні, підміна MAC-адрес та багато інших.

HIPS. Ця система зазвичай працює шляхом аналізу поведінки коду на хості, і таким чином виявляється дивна активність. HIPS надзвичайно корисний для захисту конфіденційної інформації від вилучення.

NIPS. Виявлення відбувається шляхом аналізу пакетів через мережу. Одразу після встановлення збираються дані про хост і мережу. Запобігання атакам здійснюється шляхом відхилення пакетів, обмеження пропускної здатності та TCP-з'єднань.

NBA. Цей аналіз проводиться на основі нормальної/дивної поведінки в мережі. Для того, щоб розглянути, що є нормою, а що ні, системі потрібен певний час.

HIDS. Така система необхідна для належного моніторингу ОС на пристроях або окремих хостах. Всі пакети відстежуються, щоб виявити незвичну активність. Сповіщення відбувається, коли в системі змінюються критичні файли [11].

1.3.3 Захист кінцевих точок

Кінцеві точки – це фізичні пристрої, які підключаються до комп’ютерної мережі й обмінюються з нею інформацією. Приклади кінцевих точок: настільні комп’ютери, віртуальні машини, вбудовані й мобільні пристрої та сервери. Пристрої Інтернету речей, як-от камери, холодильники, системи освітлення й безпеки, розумні динаміки та термостати, – це також кінцеві точки [12].

Кіберзлочинці атакують кінцеві точки, оскільки вони дають їм змогу легко отримувати доступ до корпоративних даних і за своєю природою вразливі до загроз. Вони захищені не системою безпеки в мережі, а окремими заходами, які впроваджують користувачі. А люди, як відомо, здатні робити помилки. В умовах розподіленої роботи, коли офісні, віддалені й гібридні працівники використовують усе більше пристроїв у різних країнах світу, захищати кінцеві точки від атак стало ще складніше.

Що більше працівників стають мобільнішими, то вразливішими стають організації до загроз для захисту кінцевих точок. Нижче наведено найпоширеніші

ризики для захисту кінцевих точок. Фішинг – це тип соціотехнічної атаки, за якого кіберзлочинці обманом змушують жертв передавати їм делікатну інформацію. Зловмисні програми з вимогою викупу – це тип шкідливого програмного забезпечення, за якого блокується доступ жертви до даних, доки вона не сплатить викуп. Основна причина порушень безпеки даних в організаціях – це втрата пристроїв. Утрата або викрадення пристроїв також може призвести до значних нормативних штрафів. Застарілі виправлення, які роблять системи вразливими та дають зловмисникам змогу проникати в них і викрадати дані. Шкідливе рекламне програмне забезпечення – це тип зловмисної програми, принцип дії якої полягає у використанні онлайн-реклами для поширення атаки й ураження систем. Атаки тіньового завантаження – автоматичне завантаження програмного забезпечення на пристрій без відома користувача [12].

Система захисту кінцевих точок включає низку процесів, служб і рішень, які вбезпечують їх від кіберзагроз. Першим інструментом для убезпечення кінцевих точок стало традиційне програмне забезпечення для захисту від вірусів і зловмисних програм. Воно запобігало завданню шкоди пристроям, мережам і службам із боку кіберзлочинців. Відтоді система захисту кінцевих точок удосконалилася та включає розширені хмарні й комплексні рішення, які допомагають виявляти, розслідувати та усувати загрози, а також керувати програмами, пристроями й користувачами [12].

1.3.4 Багатофакторна автентифікація (MFA)

Багатофакторна аутентифікація – це метод аутентифікації (ідентифікації), який вимагає від користувача надання двох або більше доказів особистості, щоб отримати доступ і увійти у свій обліковий запис. І тільки після введення всієї цієї необхідної інформації Ви отримаєте доступ до свого облікового запису. Це може бути номер телефону, адреса електронної пошти або відповідь на якесь (відоме лише Вам) секретне питання [13].

Хоча MFA об’єднує будь-яку кількість факторів аутентифікації, найбільш поширеним з них є двофакторна аутентифікація (2FA). Необхідність MFA також

може бути викликана невдалою ідентифікацією у 2FA або підозрілими діями передбачуваної особистості.

Це характерно для систем 2FA, здатних переходити у MFA. Це може також знадобитися для забезпечення додаткової безпеки при доступі до більш важливих файлів або конфіденційних даних, таких як медичні або фінансові записи. Тобто звичайна 2FA, наприклад, може надавати доступ до всіх соціальних мереж, а MFA до Ваших медичних або фінансових даних [13].

В концепції MFA існують 3 основні фактори автентифікації, серед яких [14]:

- Фактор знання (те, що ви знаєте). Це може бути пароль, пін-код або відповідь на секретне питання. Фактор є найбільш поширеним та доступним, але його безпека може бути порушена, якщо пароль стає відомим зловмисникам.

- Фактор власності (те, що ви маєте). Це може бути фізичний токен, такий як USB-ключ або мобільний телефон, на якому встановлено спеціальний захищений додаток. Фактор зазвичай надійніший, оскільки зловмисник мусить мати доступ до фізичного пристрою, щоб отримати доступ.

- Фактор приналежності (те, чим ви є). Це може бути біометричний фактор, такий як відбиток пальця, розпізнавання обличчя, голосовий або смартритм. Фактор зазвичай надійніший, оскільки біометричні дані не можуть бути викрадені або відтворені.

Кожен з цих факторів має свої переваги та недоліки. Використання більше, ніж одного фактора автентифікації забезпечує вищий рівень безпеки, оскільки зловмиснику потрібно пройти крізь кілька факторів, щоб отримати доступ до ресурсу [14].

1.3.5 Системи моніторингу безпеки (SIEM)

Системи моніторингу безпеки, також відомі як системи управління інформацією та подіями безпеки (SIEM), є інструментами, які збирають, аналізують та моніторять дані безпеки з різних джерел у мережі організації. Ці

системи забезпечують реальний час видимості подій безпеки, що дозволяє виявляти потенційні загрози, атаки та незвичайні дії [15].

Системи моніторингу безпеки відіграють критичну роль у підтримці безпеки організації. Вони збирають дані з мережевих пристроїв, серверів, додатків та засобів безпеки та агрегатують їх у централізованому місці. Потім дані аналізуються за допомогою передових алгоритмів та правил для виявлення шаблонів або аномалій, які можуть вказувати на загрозу безпеці. Ці системи використовують різні методи для моніторингу та аналізу подій безпеки, включаючи:

- Управління логами: Системи моніторингу безпеки збирають дані логів з різних джерел, таких як фаєрволи, системи виявлення та запобігання вторгнень і антивірусні програми. Вони опрацьовують та нормалізують ці логи, щоб забезпечити послідовний та точний аналіз.
- Кореляція та аналіз: Після збору даних системи моніторингу безпеки корелюють події у реальному часі, дозволяючи аналітикам безпеки зрозуміти взаємозв'язок між різними діями. Аналізуючи дані в контексті, ці системи можуть виявляти підозрілі поведінки, які можуть вказувати на порушення безпеки.
- Інтеграція з розвідкою загроз: Багато систем моніторингу безпеки інтегруються з зовнішніми каналами розвідки загроз, які надають актуальну інформацію про відомі загрози та вразливості. Ця інтеграція підвищує можливості виявлення системи, дозволяючи їй порівнювати активність у мережі з базою даних відомих зловмисних індикаторів.
- Створення сповіщень та звітів: Системи моніторингу безпеки генерують сповіщення та звіти на основі заздалегідь визначених правил та порогів. Ці сповіщення надсилаються працівникам з безпеки, які можуть розслідувати та реагувати на потенційні інциденти безпеки оперативно. Звіти надають інформацію про загальний стан безпеки організації та допомагають дотримуватися нормативних вимог щодо приватності та безпеки даних [15].

1.4 Міжнародний досвід забезпечення кібербезпеки

1.4.1 Вплив кіберзагроз на державні інститути, економіку та суспільну стабільність

У сучасному світі цифрові технології стали невід'ємною частиною функціонування державних інститутів, економічних систем та повсякденного життя громадян. Зростаюча залежність від інформаційних систем та мереж робить держави вразливими до нових загроз у кіберпросторі, де кібератаки можуть стати інструментом політичного, економічного та військового тиску. Захист критичних інформаційних інфраструктур, забезпечення безпеки даних та протидія кібератакам стають пріоритетними завданнями кожної держави, що прагне зберегти стабільність та безпеку на національному рівні [16].

З кожним роком масштаби кіберзагроз лише зростають. Наприклад, кібератака на Colonial Pipeline у 2021 році, що спричинила зупинку постачання пального в США, показала, наскільки вразливою може бути інфраструктура держави до цифрових загроз. Це доводить, що навіть розвинені країни можуть стати жертвами кібернападів, які мають серйозні економічні та соціальні наслідки. Іншим прикладом є атака вірусу NotPetya у 2017 році, яка зачепила кілька країн, включно з Україною, де в результаті були паралізовані робота банківської системи, енергетичні об'єкти та державні установи. Це підкреслює глобальний характер кіберзагроз, які можуть охоплювати як державні, так і приватні структури. У цьому контексті система кібербезпеки стає важливою складовою загальної стратегії національної безпеки держави, забезпечуючи захист її критичних ресурсів та інтересів у цифровому просторі [16].

Кібербезпека є фундаментальною складовою національної безпеки, яка відіграє важливу роль у захисті державних інтересів в умовах глобалізації та стрімкого розвитку інформаційних технологій. Визначення кібербезпеки охоплює широкий спектр аспектів, що стосуються захисту інформаційних систем, кіберпростору, а також забезпечення конфіденційності, цілісності та доступності даних. Кібербезпека визначається як система заходів, спрямованих на захист від

кіберзагроз, які можуть бути спрямовані як на державні установи, так і на приватні інституції, критичну інфраструктуру та суспільство в цілому. Згідно з визначенням, кібербезпека передбачає управління ризиками, пов'язаними з використанням цифрових технологій, та захист інформаційного середовища від несанкціонованого доступу, кібернападів та інших загроз [17].

Зв'язок між кібербезпекою та національною безпекою є очевидним і критичним. У сучасному світі національна безпека залежить не лише від фізичного захисту кордонів, але й від захисту кіберпростору, оскільки більшість державних функцій і комунікацій здійснюються за допомогою інформаційних технологій. Кіберзагрози можуть підривати функціонування державних інститутів, впливати на політичну стабільність і безпосередньо загрожувати національній безпеці. У такому контексті кібербезпека стає невід'ємною частиною національної стратегії безпеки, що охоплює як оборонні, так і наступальні аспекти кібердій. Це передбачає не лише захист державних ресурсів, але й активну протидію зовнішнім загрозам та кібертероризму.

Вплив кіберзагроз на державні інститути, економіку та суспільну стабільність є значним. Сучасні кібератаки можуть паралізувати державні системи та викликати серйозні збої в економіці. Після кібератак в Естонії у 2007 році багато країн усвідомили важливість кібербезпеки для національної безпеки. Невідомий та невидимий супротивник може завдати шкоди без прямого військового втручання, що робить кібербезпеку пріоритетом для державних стратегій безпеки. Також, атака вірусу "Petya" у 2017 році паралізувала роботу численних українських державних установ, банків і приватних компаній, що показує вразливість держави перед кіберзагрозами. Такі атаки можуть не тільки знищити важливі дані, але й дестабілізувати політичну ситуацію, створюючи недовіру до уряду з боку населення. Це підкреслює важливість створення національної системи кібербезпеки, яка повинна інтегрувати як державні, так і приватні сектори у боротьбі з кіберзагрозами [18].

У світі спостерігається тенденція до підвищення уваги до кібербезпеки з боку міжнародних організацій. Провідні країни світу вже розробили стратегії кібербезпеки, які включають не тільки захист інформаційних систем, але й заходи щодо попередження кібершпигунства та кібертероризму [18]. Кіберзагрози мають багатогранний вплив на різні сфери державного та суспільного життя, так, кібератаки можуть призвести до витоку конфіденційної інформації, порушення роботи урядових систем та підриву довіри громадян до державних установ. Кіберзлочинність завдає значних фінансових збитків компаніям та державі. Атаки на фінансові установи, промислові підприємства та інші економічно важливі об'єкти можуть призвести до економічної нестабільності. Поширення дезінформації та маніпуляція громадською думкою через кіберпростір можуть викликати соціальні напруження, політичну нестабільність та підривати демократичні процеси. У зв'язку з цим, забезпечення кібербезпеки є критично важливим для захисту національних інтересів та підтримки стабільності держави. Кібербезпека є ключовим елементом національної безпеки в інформаційному суспільстві. Захист від кіберзагроз вимагає комплексного підходу, що включає міжнародну співпрацю, розвиток законодавчої бази та впровадження передових технологій [18].

1.4.2 Політика та стратегія кібербезпеки ЄС та США

Ключовим документом у захисті від кіберзагроз є Конвенція Ради Європи про кіберзлочинність, ратифікована в 2005 році. Її метою є підвищення ефективності кримінальних розслідувань та судового переслідування, пов'язаних з комп'ютерними системами та даними, шляхом спрощення процедури збору електронних доказів. Частина дослідників виступає за прийняття на рівні ООН універсального міжнародно-правового акта, подібного до Конвенції проти кіберзлочинності, для врегулювання питань міжнародної співпраці у боротьбі з кіберзагрозами. Однак інші фахівці вважають, що механізмів, передбачених Конвенцією Ради Європи 2001 року, достатньо для ефективної протидії кіберзлочинності. Ці механізми спрямовані на вдосконалення кримінальних розслідувань, судового переслідування та полегшення збору електронних доказів.

Європейський Союз був і залишається зразком кращих практик розробки і впровадження спільної політики у різних сферах життєдіяльності як на рівні Європейської спільноти, так і на рівні держав-членів. Формування політики кібербезпеки не є винятком. Однак, політика кібербезпеки ЄС пройшла нелегкий шлях вдосконалення й адаптації під умови мінливого цифрового середовища, ландшафту кіберзагроз і динамічних викликів новітніх технологій [19].

Розглянемо еволюцію політики кібербезпеки ЄС на основі аналізу нормативно-правових актів ЄС (табл. 1.2) [19].

Таблиця 1.2

Основні нормативно-правові акти, що регламентують питання кібербезпеки ЄС

Рік	Назва нормативно-правового документа
1995	Директива про захист осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних
1999	Ініціатива «Електронна Європа» та План дій щодо її реалізації
2000	Спільна позиція про переговори щодо конвенції Ради Європи про кіберзлочинність
2001	Повідомлення щодо створення безпечного інформаційного суспільства
	Повідомлення щодо безпеки мереж та інформації (NIS)
	Конвенція про кіберзлочинність
	Регламент про захист осіб у зв'язку з обробкою персональних даних
2002	Резолюція щодо спільного підходу і конкретних дій у сфері NIS
2004	Регламент про створення ENISA
2005	Рамкове рішення щодо атак проти інформаційних систем
2006	Стратегія безпечного інформаційного суспільства
2009	Повідомлення про захист критичної інформаційної інфраструктури: захист від масштабних кібератак і збоїв через посилення готовності, безпеки і стійкості
2013	Стратегія кібербезпеки ЄС «Відкритий, надійний і безпечний кіберпростір»
	Директива ЄС про атаки на інформаційні системи
2016	Глобальна стратегія із зовнішньої і безпекової політики ЄС
	Директива з безпеки мережевих та інформаційних систем NIS
	Загальний регламент про захист даних (GDPR)
2017	Стратегія кібербезпеки «Стійкість, стримування та захист: побудова міцної кібербезпеки для ЄС»
2019	Регламент про ENISA і сертифікацію ІКТ в галузі кібербезпеки (Акт з кібербезпеки)
2020	Стратегія кібербезпеки ЄС для цифрового десятиліття
2022	Директива щодо заходів для забезпечення високого спільного рівня кібербезпеки в ЄС (NIS 2)
	Регламент щодо заходів для високого загального рівня кібербезпеки в органах ЄС
	Регламент щодо горизонтальних вимог кібербезпеки для продуктів із цифровими елементами (Акт про кіберстійкість) — *проєкт*
2023	Регламент щодо заходів посилення солідарності й потужностей ЄС з метою виявлення, підготовки та реагування на загрози й інциденти кібербезпеки (Акт про кіберсолідарність) — *проєкт*

Основи політики кібербезпеки ЄС були закладені у кінці 90-х років минулого століття. Реагуючи на виклики, пов'язані з розбудовою цифрового суспільства й упровадження ІКТ, керівництво ЄС акцентувало на важливості мережевої безпеки й боротьби з кіберзлочинністю, зокрема зробило низку кроків для боротьби зі шкідливим і незаконним контентом в Інтернеті, захисту інтелектуальної власності й персональних даних, сприяння електронній торгівлі та підвищення безпеки транзакцій [19].

Починаючи з початку 2000-х років, Європейська Комісія починає приділяти все більше уваги питанням кібербезпеки. Водночас, основні зусилля зосереджуються на питаннях удосконалення інформаційної інфраструктури, захисту даних і протидії комп'ютерній злочинності [19].

Слід відзначити, що саме в цей час у законодавстві ЄС почали використовувати термін «мережева та інформаційна безпека» (Network and Information Security, NIS), під якою розуміють здатність мережі або інформаційної системи протистояти випадковим подіям або зловмисним діям на заданому рівні довіри [19].

Також Єврокомісія окреслила спільний підхід до європейської політики NIS, який передбачав подальшу реалізацію заходів за такими напрямами: обгрунтування політики і вдосконалення нормативно-правової бази; створення європейської системи попередження та інформування; підтримка й інвестування в технологічні рішення NIS; підвищення обізнаності; підтримка ринково орієнтованої стандартизації та сертифікації; забезпечення безпеки інституцій ЄС і країн-членів; міжнародна співпраця [19]. Держави-члени ЄС отримали вказівки щодо впровадження відповідних рішень на національному рівні [19].

Наступним важливим кроком у розбудові європейської політики кібербезпеки, зокрема її інституційної складової, стало створення у 2004 році Європейського агентства мережевої та інформаційної безпеки ENISA [19], яке відігравало і продовжує відігравати ключову роль у забезпеченні кібербезпеки Спільноти. На той час ENISA отримало повноваження щодо консультування

інституцій ЄС з питань NIS, сприяння підвищенню обізнаності й обміну кращими практиками, посилення співпраці з усіма зацікавленими сторонами у цій сфері, а також відстеження розробки стандартів для продуктів і послуг NIS і управління кіберризиками.

Усвідомлюючи необхідність об'єднання зусиль державного і приватного секторів у подоланні спільних проблем кібербезпеки, Єврокомісія розпочала налагодження тісної співпраці з економічними гравцями, запросивши зацікавлених представників приватного сектора взяти участь у поширенні кращих практик безпеки; визначенні вимог безпеки для виробників ПЗ і провайдерів Інтернет-послуг; впровадженні навчальних програм з безпеки для персоналу, здійсненні сертифікації безпеки для продуктів, процесів і послуг тощо [19].

Новий етап розвитку політики кібербезпеки ЄС ознаменувався прийняттям у 2013 році першої Стратегії кібербезпеки ЄС «Відкритий, надійний і безпечний кіберпростір», у якій кібербезпека була визнана новим окремим напрямом політики ЄС. Під кібербезпекою Стратегія розуміє заходи безпеки та дії, які можуть бути використані для захисту кіберсередовища, як у цивільній, так і у військовій сферах, від тих загроз, які пов'язані або можуть зашкодити його взаємозалежним мережам та інформаційній інфраструктурі. Метою кібербезпеки визначено збереження доступності й цілісності мереж та інфраструктури, а також конфіденційності даних, які в них містяться [19].

Відповідно до Стратегії принципами кібербезпеки є: застосування у кіберпросторі тих же цінностей, законів і норм, що і в фізичному світі, захист основних прав, свободи вираження поглядів, персональних даних і конфіденційності; забезпечення необмеженого і безпечного доступу до Інтернету для всіх; демократичне й ефективне багатостороннє управління Інтернетом; спільна відповідальність за кібербезпеку.

Стратегічними пріоритетами ЄС було визначено:

- досягнення кіберстійкості, яке передбачає розбудову можливостей держав-членів ЄС шляхом встановлення загальних мінімальних вимог до кібербезпеки на національному рівні, зокрема призначення національних компетентних органів,

прийняття національної стратегії і плану дій з кібербезпеки, створення CERT; створення узгоджених механізмів запобігання, виявлення, пом'якшення та реагування у сфері кібербезпеки; підвищення готовності й залучення приватного сектору, а також зростання обізнаності користувачів з питань кібербезпеки;

- значне скорочення кіберзлочинності, яке має бути досягнене шляхом формування сильного й ефективного законодавства щодо протидії кіберправопорушенням; розширення й оновлення оперативного потенціалу для боротьби з кіберзлочинністю (застосування новітніх засобів і методів, збір і поширення передового досвіду подолання кіберзлочинності у співпраці з Європейським центром боротьби з кіберзлочинністю ЕС3 та Євроюстом); покращення координації зусиль з метою протидії кіберзлочинності на рівні ЄС;
- розробку політики кіберзахисту, що охоплює оцінювання оперативних вимог і розробку основ політики кіберзахисту ЄС, покращення можливостей освіти й навчання з кіберзахисту для військових, сприяння діалогу та координації між цивільними та військовими суб'єктами в ЄС щодо раннього попередження, реагування на інциденти, оцінювання ризиків тощо; забезпечення діалогу з міжнародними партнерами для забезпечення ефективного кіберзахисту;
- розвиток промислових і технологічних ресурсів для кібербезпеки, яке буде здійснюватися через розвиток єдиного ринку для продуктів кібербезпеки, з одного боку, мотивування виробників і провайдерів послуг забезпечувати високі стандарти безпеки, з іншого — стимулювання ринкового попиту на «високо безпечні» продукти в ЄС, розробка галузевих стандартів і сприяння добровільній сертифікації з кібербезпеки, введення т.зв. «міток безпеки» для кращих компаній; інвестування в дослідження і сприяння інноваціям;
- формування узгодженої міжнародної політики в кіберпросторі для ЄС та просування основних цінностей спільноти, таких як людська гідність, свобода, демократія, рівність, верховенство права та повага до основних прав людини, що охоплюватиме зусилля ЄС зі сприяння відкритості та свободі Інтернету, розробки норм поведінки й застосування чинних міжнародних законів у кіберпросторі, усунення цифрового розриву і створення потенціалу кібербезпеки [19].

Директиву ЄС про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (2016 рік) та Директиву ЄС щодо боротьби з шахрайством та іншими фінансовими злочинами в Інтернеті (2017 рік). Особлива увага в ЄС приділяється своєчасному виявленню та швидкому реагуванню на кіберінциденти й атаки на електронні інформаційні ресурси. Директива ЄС про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу, ухвалена в 2016 році, стала важливим кроком у зміцненні кібербезпеки всередині Європейського Союзу [18].

Основною метою цієї директиви було встановлення єдиних стандартів безпеки для мережевих та інформаційних систем у державах-членах ЄС. Вона зобов'язала країни створити національні органи, відповідальні за кібербезпеку, та визначити конкретні сектори, критично залежні від інформаційних систем, включаючи енергетику, транспорт, банківську сферу, охорону здоров'я та водопостачання. Директива також запровадила вимогу до операторів основних послуг та провайдерів цифрових послуг повідомляти про серйозні інциденти в своїй інфраструктурі, що дозволяє швидко реагувати на загрози. Одним з аспектів директиви є стимулювання міжнародного співробітництва в сфері кібербезпеки та обмін інформацією між державами-членами для забезпечення колективної кібербезпеки на рівні ЄС.

Директива Європейського Союзу щодо боротьби з шахрайством та іншими фінансовими злочинами в Інтернеті, ухвалена в 2017 році, спрямована на боротьбу з кіберзлочинністю, пов'язаною з фінансовими операціями в цифровому просторі. Вона встановлює правову основу для запобігання та протидії фінансовим злочинам в Інтернеті, включаючи крадіжки даних, незаконне використання платіжних засобів, фішинг та інші форми онлайн- шахрайства. Основна увага цієї директиви зосереджена на захисті електронних транзакцій та платіжних систем від кіберзлочинців. Директива також вимагає від держав-членів забезпечити жорстке покарання за кіберзлочини, пов'язані з фінансовими операціями, та стимулювати міжнародну співпрацю для швидкого реагування на загрози в цій сфері. Особливий акцент робиться на забезпеченні безпеки особистих даних

користувачів під час фінансових операцій і вдосконаленні механізмів обміну інформацією між країнами щодо кіберзагроз [18].

Початком поточного етапу розвитку політики кібербезпеки ЄС стало прийняття у 2020 році Стратегії кібербезпеки ЄС на цифрове десятиліття [19]. Стратегія декларує прагнення ЄС щодо забезпечення глобального та відкритого Інтернету з надійними бар'єрами для усунення ризиків безпеці й основним європейським цінностям, і містить пропозиції щодо застосування трьох основних інструментів: регуляторних, інвестиційних і політичних, — для досягнення трьох цілей ЄС (рис.1.1) [19].

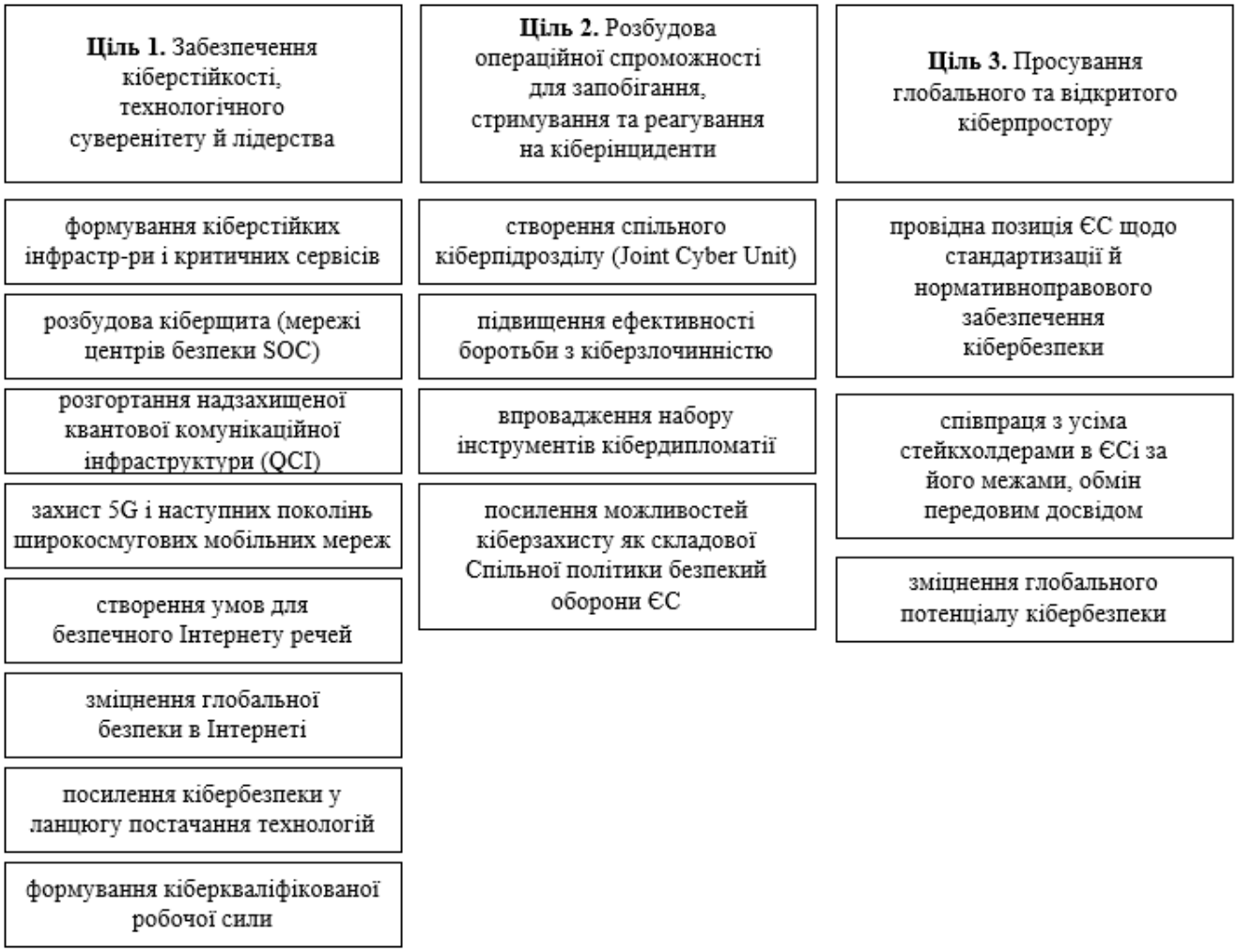

Рис. 1.1 Цілі й завдання Стратегії кібербезпеки ЄС на цифрове десятиліття

Порівняння положень Стратегій 2020 і 2017 років показало, що цілі практично накладаються: перша ціль має на меті забезпечення стійкості до кібератак; друга - стримування кіберзлочинності й кіберзахист; третя - об'єднання зусиль усіх зацікавлених сторін (як в ЄС, так і по всьому світу; державних,

приватних, експертних організацій та громадян) для формування безпечного кіберпростору.

Натомість, для досягнення кожної з цілей у Стратегії 2020 року передбачено низка принципово нових конкретних завдань, які раніше не окреслювалися в основоположних нормативних документах ЄС [19].

Так, забезпечення кіберстійкості, технологічного суверенітету й лідерства має бути досягнуте, зокрема, шляхом:

- формування кіберстійких інфраструктури і критичних сервісів в результаті реформування вимог щодо безпеки і звітності про інциденти, національного нагляду та правозастосування для стратегічно важливих секторів, а також зміцнення кіберстійкості демократичних процесів та інституцій;
- розбудови єдиної мережі операційних центрів безпеки (SOC), щоб завдяки використанню штучного інтелекту й машинного навчання завчасно виявляти ознаки неминучих кібератак і вживати запобіжних заходів;
- розгортання надзахищеної квантової комунікаційної інфраструктури (QCI);
- захист 5G і наступних поколінь широкосмугових мобільних мереж;
- створення умов для Інтернету безпечних речей, зокрема через впровадження прозорих рішень безпеки й сертифікації;
- посилення кібербезпеки ланцюжка постачання технологій, включаючи дані та хмари, процесорні технології нового покоління, надбезпечне під'єднання та мережі 6G;
- формування кіберкваліфікованої робочої сили шляхом залучення, утримання, розвитку й підвищення кваліфікації спеціалістів із кібербезпеки, інвестування в дослідження та інновації світового класу, що має сприяти подальшому збільшенню навичок кібербезпеки та кіберзахисту на рівні ЄС;
- зміцнення глобальної безпеки в Інтернеті через розробку плану на випадок надзвичайних ситуацій (зловмисних кібератак, великих геополітичних і технічних інцидентів), які можуть вплинути на цілісність і доступність глобальної кореневої системи DNS, впровадження ключових стандартів Інтернету та безпеки мережі [19].

У рамках розбудови операційної спроможності для запобігання, стримування та реагування на кіберінциденти передбачено створення спільного кіберпідрозділу (Joint Cyber Unit), який має забезпечити оперативну й технічну координацію щодо протидії великим транскордонним кіберінцидентам і загрозам; посилення можливостей кіберзахисту шляхом розробки й використання технологій штучного інтелекту, шифрування та квантових обчислень, а також забезпечення синергії кіберзусиль між цивільною, оборонною і космічною галузями; впровадження набору інструментів кібердипломатії для посилення дипломатичної відповіді ЄС на дії у кіберпросторі, які несуть потенційну шкоду інтересам європейської спільноти [19].

Досягнення цілі з просування глобального та відкритого кіберпростору охоплює виконання завдань щодо стандартизації новітніх технологій (штучний інтелект, хмарні обчислення, квантові обчислення й комунікації); захисту правозахисників, громадянського суспільства й наукових кіл, які працюють над вирішенням проблем кібербезпеки, конфіденційності даних, стеження й онлайн-цензури.

Особливий акцент зроблено на посиленні співпраці та забезпечення захисту основних прав і свобод, зокрема права на гідність, приватне життя і свободу вираження поглядів та інформації у всесвітній мережі, а також пошуку моделі багатостороннього управління Інтернетом [19].

ЄС зобов'язався підтримувати цю Стратегію шляхом безпрецедентного рівня інвестицій у цифровий перехід ЄС протягом наступних 7-ми років, перевищивши попередні рівні фінансування кібербезпеки в чотири рази [19].

Упродовж 2022–2023 років Єврокомісія запропонувала низку важливих ініціатив, спрямованих на досягнення стратегічних цілей посилення кібербезпеки і кіберстійкості Європейського Союзу і держав-членів.

Так, для забезпечення високого спільного рівня кібербезпеки в ЄС Єврокомісія зобов'язала держави ЄС прийняти національні стратегії кібербезпеки та призначити або створити компетентні органи, органи управління кіберкризами, єдині контактні пункти з питань кібербезпеки і групи реагування на інциденти

комп'ютерної безпеки CSIRT; підвищити рівень гармонізації вимог безпеки, забезпечити реалізацію заходів базового рівня з управління ризиками кібербезпеки і встановити зобов'язання щодо звітності для організацій критичних і важливих галузей; забезпечити виконання організаціями правил і зобов'язань щодо обміну інформацією у сфері кібербезпеки. За невиконання зазначених вимог передбачені штрафні санкції, обсяг яких залежить від тяжкості порушення розміру організації. На виконання вказівок Єврокомісії була створена Європейська мережа національних CSIRT і офіційно розпочала роботу мережа національних органів держав-членів, які відповідають за управління кіберкризами (European Cyber Crisis Liaison Organisation Network, EU-CyCLONe) [19].

З огляду на посилення ризиків кібербезпеки і зростання вразливості інституцій ЄС до кіберзагроз та інцидентів запроваджено загальні стандарти кібербезпеки щодо створення структур управління безпекою й оцінки ризиків, розробки планів удосконалення кібербезпеки; розширено можливості й фінансування CERT-EU, яка здійснює нагляд за станом кібербезпеки установ та організацій Євросоюзу; передбачено створення міжвідомчого органу з безпеки (Interinstitutional Cybersecurity Board), який стежитиме за реалізацією зазначених вимог. Також було узгоджено часові рамки для звітування про серйозні кіберінциденти [19].

Продовжуючи зусилля щодо розвитку безпечного й надійного єдиного цифрового ринку ЄС, у кінці 2022 року Єврокомісія внесла проєкт Регламенту щодо горизонтальних вимог кібербезпеки для продуктів із цифровими елементами (Акт про кіберстійкість, Cyber Resilience Act, CRA) [19], який спрямований на вирішення проблем неналежного рівня кібербезпеки цифрових продуктів, або неадекватного оновлення їхньої безпеки, а також відсутності у споживачів і компаній можливості визначити, які продукти є кіберзахищеними і вартими довіри.

Регламент вводить обов'язкові вимоги кібербезпеки протягом усього ланцюжка поставок і життєвого циклу апаратних і програмних продуктів (проєктування, розробки, виробництва та продажу), щоб уникнути дублювання

вимог у різних нормативно-правових актах держав-членів ЄС, заповнити існуючі прогалини у чинному законодавстві про кібербезпеку ЄС і зробити його більш послідовним і узгодженим.

Відповідальність за дотримання нормативних вимог безпеки покладено на виробників, які зобов'язані проводити оцінку ризиків кібербезпеки для продуктів із цифровими елементами, доступними на ринку ЄС, декларувати дотримання відповідності та співпрацювати з відповідними компетентними органами ЄС. Також у Регламенті окреслено основні вимоги та зобов'язання виробників цифрових продуктів щодо процесів обробки кіберуразливостей, окреслено заходи щодо підвищення прозорості безпеки апаратних і програмних продуктів для споживачів і бізнес-користувачів, а також визначено структуру нагляду за ринком для забезпечення дотримання цих правил [19].

У листопаді 2023 року Рада ЄС і Європарламент досягли попередньої угоди щодо Регламенту про кіберстійкість, а в березні 2024 року Європарламент схвалив його зі змінами, внесеними за результатами дебатів. Щоб набути чинності, Регламент має бути офіційно прийнятий Радою ЄС [19].

Регламент про кіберстійкість стане першим у світі нормативним актом, який визначає вимоги безпеки для продуктів як перешкоду для входу на ринок. Обмеження почнуть діяти з 2027 року [19].

В умовах глобального протистояння та мілітаризації кіберпростору, США залишаються провідною силою у формулюванні та впровадженні кібербезпекової стратегії. Вони підкреслюють важливість національної безпеки через кіберзахист. Стратегія кібербезпеки, опублікована урядом США, визначає кібербезпеку як комплекс заходів для захисту комп'ютерних систем від несанкціонованого доступу. Важливим аспектом є регулювання безпеки на національному рівні, включаючи застосування санкцій та стратегічні партнерства з іншими країнами для спільної боротьби проти кіберзагроз. США активно співпрацюють з країнами-партнерами, такими як Україна, у сфері вдосконалення кібербезпеки.

Нормативні документи, що визначають ключові принципи національної безпеки та оборони, такі як Доктрина інформаційної безпеки та Стратегічний

оборонний бюлетень, підкреслюють важливість міжнародної співпраці. Розвиток партнерських відносин з іноземними, цивільними та військовими організаціями сприяє обороноздатності та державній безпеці. Це стимулює вітчизняних фахівців до вдосконалення національної моделі державного управління у сфері кібербезпеки на основі вивчення міжнародного досвіду.

Система кібербезпеки в сучасних країнах є складним комплексом технологічних, організаційних та законодавчих заходів. Вона спрямована на захист національних інтересів у кіберпросторі, захист критичної інфраструктури та інформаційних ресурсів від різноманітних кіберзагроз. Досвід США у цій сфері демонструє важливість комплексного підходу, міжнародної співпраці та постійного вдосконалення законодавчої бази. Для країн, що розвивають власні системи кібербезпеки, вивчення та адаптація такого досвіду є критично важливими для забезпечення національної безпеки та суверенітету в цифрову епоху. Міжнародне співробітництво у сфері кібербезпеки потребує гармонізації кримінального законодавства, розробки нових елементів міжнародного партнерства та підтримки договорів і моделей, таких як Типовий закон ООН про комп'ютерні злочини. Незважаючи на наявність усталених міжнародних конвенцій і постійних зусиль, динамічний характер кіберзагроз потребує безперервної адаптації правової бази та скоординованих дій для ефективної протидії та запобігання кіберзлочинності на глобальному рівні [18].

1.4.3 Кібертероризм

Кіберзагрози стають все складнішими і різноманітнішими. Наприклад, у 2015 році була виявлена масштабна кампанія кібершпигунства, спрямована на урядові установи різних країн, з метою викрадення дипломатичної інформації та стратегічних планів. Кібертероризм є ще одним серйозним викликом. Він передбачає використання комп'ютерних та мережевих технологій для здійснення терористичних актів або сприяння їм. Метою кібертерористів є посіяти паніку, дестабілізувати суспільство або завдати шкоди критичній інфраструктурі. Наприклад, атаки на системи управління міським транспортом можуть призвести до хаосу на дорогах, а втручання в роботу медичних закладів – до загрози життю

пацієнтів. Кібертероризм особливо небезпечний тим, що дозволяє зловмисникам діяти анонімно та з будь-якої точки світу. Атаки на критичну інфраструктуру є однією з найбільш руйнівних форм кіберзагроз [20].

У дослідженні 10Guards були виділені основні типи атак 2021 року. Фішинг – одна з найпоширеніших загроз, яка включає spear-phishing, whaling, smishing, vishing, і email phishing. Програми-вимагачі (ransomware) блокують доступ до даних і вимагають викуп. Шкідливе ПЗ (malware) шкодить пристроям та краде інформацію. Витік даних часто спричиняється через погано захищені системи. DDoS-атаки перевантажують сервери, а атаки "Людина посередині" перехоплюють комунікації. Інші загрози включають SQL-ін'єкції, експлойти нульового дня та атаки брутфорс. Організації повинні бути готові до цих загроз, впроваджуючи захисні заходи [21].

Атака на українську енергосистему 2015 року залишила понад 200 тисяч людей без електроенергії, підкресливши вразливість інфраструктури. Вірус NotPetya 2017 року вразив тисячі комп'ютерів, зокрема в Україні, спричинивши значні збитки. Атака на Colonial Pipeline у 2021 році зупинила постачання палива на східне узбережжя США, викликавши паніку і дефіцит [16]. На сьогоднішній день Україна перебуває в стані війни та потерпає від кібератак з боку росії, постійні безуспішні атаки на “Monobank”, “Privat24” та інші банки з метою викрадення даних та коштів користувачів, атака на сайти такі як “UAKino”, “UASerials” та інші з метою отримання даних користувачів, які були зареєстровані на сайті та просто задля заволодіння сайтів. Атаки на критичні інфраструктури такі як “Укренерго” з метою порушення енергосистеми та комфорту українців. Атаки на медичні заклади, застосунок eHealth та на бази вакцинації від COVID-19 з метою підриву довіри до медсистеми та, знову ж, викрадення персональних даних. Постійні атаки на сайти Міноборони та застосунки “Резерв+” та “Дія”. Втручання у вибори США 2016 та 2020 років показало, що кіберзагрози можуть мати політичні наслідки. Наслідки кібератак для національної безпеки включають економічні втрати, гуманітарні кризи, загрози життю громадян, та

ослаблення обороноздатності. Соціальні наслідки можуть включати поширення дезінформації, паніку і суспільні заворушення [16].

Для ефективної протидії кіберзагрозам необхідний комплексний підхід. Держави повинні інвестувати у розвиток національних систем кібербезпеки, створювати спеціалізовані органи та підрозділи, що відповідають за захист критичної інфраструктури та державних установ. Необхідно удосконалювати законодавчу базу, встановлюючи чіткі правила та норми поведінки в кіберпросторі. Міжнародна співпраця є ключовим елементом у боротьбі з кіберзлочинністю. Оскільки зловмисники діють глобально, без взаємодії між державами, правоохоронними органами та міжнародними організаціями ефективна протидія неможлива. Необхідно розробляти спільні стандарти безпеки, обмінюватися інформацією та досвідом, проводити спільні навчання та операції [16].

Важливим є також підвищення обізнаності громадян та приватного сектора про кіберзагрози. Проведення освітніх програм, тренінгів та кампаній з кібергігієни допоможе знизити ризик успішних атак, які часто використовують людський фактор як найслабшу ланку в системі безпеки. У підсумку, кіберзагрози є невід'ємною частиною сучасного світу і становлять серйозну загрозу для національної безпеки. Їхній вплив може бути руйнівним, але за умови правильного підходу та співпраці можливо ефективно протидіяти цим викликам. Забезпечення кібербезпеки має стати пріоритетом для держав, бізнесу та суспільства, адже від цього залежить наше спільне майбутнє у цифрову епоху [16].

Досвід іноземних країн та особливості українських реалій свідчать, що розв’язання основних завдань кібербезпеки неможливе без створення: міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки; центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення й оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад і надання

рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін і впливу на їх інформаційно-телекомунікаційні системи; органів власної інформаційної та кібербезпеки – державних установ (відомств) і комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпросторів [1][22].

Необхідно зазначити, що координаційні структури, які об'єднують і спрямовують діяльність суб'єктів забезпечення кібербезпеки, нині створені й успішно працюють вже у багатьох країнах. Так, у 2017 р. в Таллінні був створений Об'єднаний центр передових технологій із кібероборони НАТО. Центр отримав акредитацію НАТО, налічує 20 учасників – 17 членів НАТО і 3 – держави партнера. Основне завдання Центру – тренування фахівців із різних країн, які забезпечують безпеку в національному кіберпросторі. У Литві Міністерству оборони надано право координувати національну політику з кібербезпеки, передбачається установа Національного центру кібербезпеки, створення Консультативної ради з кібербезпеки при Міністерстві оборони. У Чехії у 2017 р. створено Національний офіс із кібербезпеки та інформації, до функцій якого входить вирішення проблем кібербезпеки, підтримка державних установ і підприємств в разі кібератак, профілактика злочинів у кіберпросторі, забезпечення безпеки інформаційної інфраструктури [1].

Висновки до першого розділу

В Україні, в умовах постійних кібератак, спричинених повномасштабною війною, активно розвиваються та впроваджуються сучасні технології кіберзахисту. Але є загально державна проблема забезпечення державних установ та МО України захищеним месенджером вітчизняної розробки (ЗМВР).

Зараз основними месенджерами спілкування працівників державних установ, військових переважно є Signal та WhatsApp. Всі популярні месенджери мають юрисдикцію компаній у США, Японії, Швейцарії (аналіз існуючих месенджерів із функціями безпеки буде представлено у другому розділі роботи), тому створення ЗМВР може бути пріоритетним в зв'язку з необхідністю його застосування в

секторі національної безпеки оборони і на об’єктах критичної інфраструктури України.

Згідно наказу Державної служби спеціального зв’язку і захисту інформації України від 20.07.2007 р. № 141 [43] для створення ЗМВР потрібні: Замовник та Розробник.

1. Замовник на підставі своїх вихідних даних розробляє технічне завдання (ТЗ) на розроблення ЗМВР. Замовником можуть бути органи державної влади та місцевого самоврядування, МО України, організація критичної інфраструктури тощо;

2. Розробник повинен мати:

- ліцензію на право провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації;
- нормативні документи;
- власні приміщення;
- робочі площі;
- обладнання;
- кваліфікованих працівників.

В Україні є компанії, які спеціалізуються на розробці продуктів і рішень в області криптографічного захисту інформації (КЗІ) і проводять свою діяльність у відповідності до отриманих ліцензій Державної служби спеціального зв’язку і захисту інформації України у галузі криптографічного захисту інформації. Наприклад: ТОВ «Трител» спеціалізується на створенні телекомунікаційних мереж спеціального призначення, розробці та серійному виробництві засобів спеціального зв’язку та криптографічного захисту інформації [44].

ТОВ «АВТОР» об'єднує висококваліфікованих фахівців в області інформаційної безпеки, які протягом 20 останніх років займаються розробкою і впровадженням апаратно-програмних засобів криптографічного захисту [45].

Організаційно розробник має створити правові умови для своєї діяльності, зокрема зареєструвати юридичну особу або фізичну особу-підприємця, розробити чітку політику конфіденційності та користувацьку угоду відповідно до українського законодавства. Він також повинен визначити відповідального за обробку персональних даних у разі масштабного збою інформації, забезпечити належну інфраструктуру для зберігання даних користувачів і контролювати відповідність серверних рішень вимогам інформаційної безпеки.

РОЗДІЛ 2

АНАЛІТИЧНИЙ ОГЛЯД ПОТОЧНОГО СТАНУ ЗАСТОСУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕСЕНДЖЕРІВ

2.1 Основні поняття та визначення

2.1.1 Месенджери та їх роль у сучасному інформаційному обміні

МЕСЕНДЖЕР – це програма або онлайн-сервіс для обміну миттєвими повідомленнями між користувачами. Він дозволяє надсилати текстові повідомлення, голосові повідомлення, файли, фото, відео та здійснювати аудіо та відеодзвінки.

Месенджери поділяються на декілька типів такі, як текстові, корпоративні або ж вбудовані месенджери в соціальних мережах. Найпоширеніший вид – текстові месенджери, прикладами таких є Telegram, WhatsApp, Threema, QQ, WeChat. Текстові месенджери дозволяють обмінюватися голосовими та текстовими повідомленнями, фото та відео. Вбудовані месенджери дозволяють користувачам спілкуватися безпосередньо в самих соціальних мережах, прикладами таких месенджерів є Facebook Messenger або Instagram. Корпоративні мережі потрібні більш для офісів так як вони створені для організації роботи в команді та загалом мають функції для ділового спілкування, графіки, календарі роботи та інше. Прикладами корпоративних мереж є Ringostat, Slack або Leverice.

Популярність месенджерів зумовлена їх швидкістю відправки повідомлень порівняно з електронною поштою або листоношою. Більшість месенджерів безкоштовні або мають незначну плату за їх додаткові функції. Функціональність месенджерів, а саме відеодзвінки, запис та відправка голосових повідомлень, створення опитувань або відправка файлів фото та відео роблять месенджери ще більш корисними.

У 2025 році ринок месенджерів продовжує активно розвиватися, пропонуючи користувачам різноманітні платформи для спілкування. За останніми даними з відкритих джерел, у 2025 році світовий рейтинг месенджерів виглядає так:

WhatsApp – 2,9 млрд користувачів, Facebook Messenger – 1 млрд користувачів, WeChat – 1,3 млрд користувачів, QQ – 648 млн користувачів, Telegram – 900 млн користувачів, Snapchat – 750 млн активних користувачів на місяць [23] (рис. 2.1).

Рис. 2.1 Популярність месенджерів у світі (2024-2025)

WhatsApp – пропрієтарний месенджер для смартфонів. Дозволяє пересилати текстові повідомлення (дописи), зображення, відео та аудіо. Клієнт працює на платформах Android (окремих версіях), iOS, Series 40, Symbian (S60) і Windows Phone. Компанію, яка створила месенджер, заснували у 2009 році американський програміст українсько-єврейського походження Ян Кум з міста Фастова Київської області (Україна) і Браян Ектон у місті Санта-Клара, штат Каліфорнія (США). У лютому 2014 року Facebook оголосив про намір придбати WhatsApp, у жовтні 2014 року операцію з придбання мобільного месенджера WhatsApp вартістю 19 млрд $ – було завершено [24].

Особливості WhatsApp представляють собою простий інтерфейс, наскрізне шифрування повідомлень за замовчуванням, можливість обміну текстовими повідомленнями, голосовими та відеодзвінками. Месенджер має велику базу користувачів та активну підтримку різних функцій - функція захисту IP-адрес під

час дзвінків, функції повідомлень, котрі зникають, і обмеженого редагування повідомлень [23]. На рис. 2.2 зображено приклад інтерфейса WhatsApp.

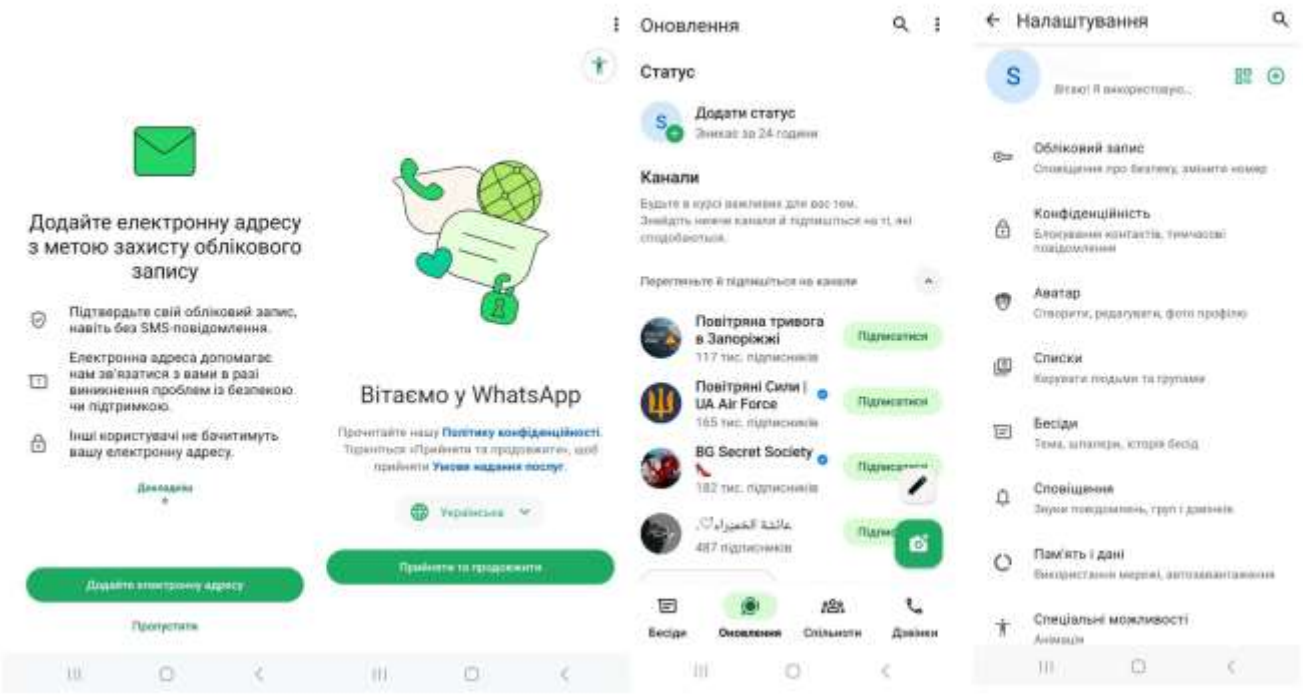

Рис. 2.2 Інтерфейс WhatsApp

Facebook Messenger – система обміну миттєвими повідомленнями, створена Facebook. Інтегрована з додатком на основному сайті Facebook і побудована на базі відкритого протоколу MQTT. Безкоштовний мобільний застосунок для обміну повідомленнями, який використовується для обміну миттєвими повідомленнями, обміну фотографіями, відео, аудіозаписами та для групових чатів. Застосунок можна використовувати для спілкування зі своїми друзями у Facebook та з телефонними контактами [25]. На рис. 2.3 зображено приклад інтерфейсу Facebook Messenger.

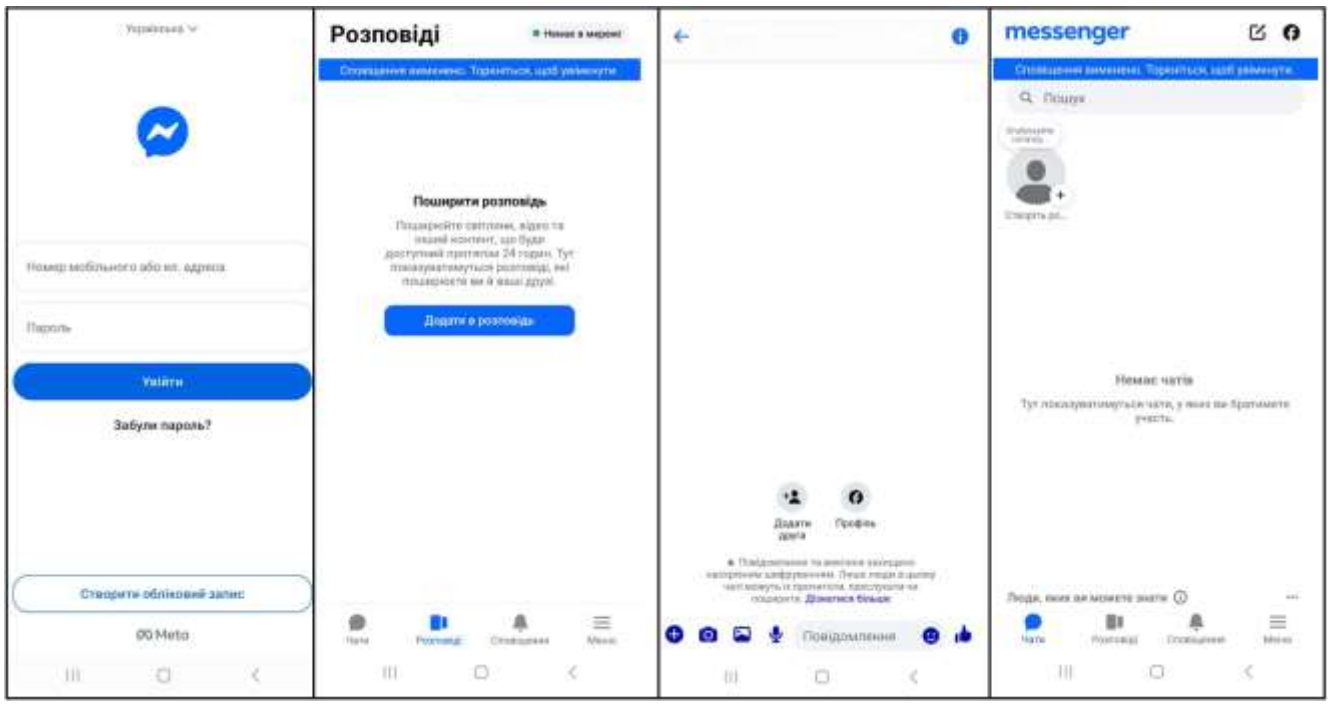

Рис. 2.3 Інтерфейс Facebook Messenger

Особливостями Facebook Messenger є інтеграція з Facebook, підтримка чат-ботів, можливість обміну мультимедійними файлами та відеодзвінків.

Snapchat – месенджер, який дозволяє обмінюватись повідомленнями, фото та відео. Створений Еваном Шпігелем, Боббі Мерфі та Реджі Брауном під час навчання в Стенфордському університеті [26].

Основні плюси месенджера це – зникаючі повідомлення, які зникають протягом 24 годин після відправлення. Додаток сповіщає користувача, якщо співрозмовник зробив скріншот листування, приватність акаунту – тільки контакти, які ви додали до себе можуть надсилати вам повідомлення, є можливість скрити профіль для додавання, тобто профіль не буде відображений в пошуку іншим користувачам. Має двохфакторну аутентифікацію (2FA).

WeChat – мобільна платформа для обміну текстовими та голосовими повідомленнями, розроблена компанією Tencent. Додаток доступний для усіх популярних мобільних платформ, має версію для ПК та веб (що потребує аутентифікації через мобільний додаток). WeChat дає змогу ділитися фото та відео, робити масові розсилки, обмінюватися контактами через Bluetooth,

підтримуються QR-коди для швидкого додання контакту, обробка фотографій фільтрами, а також сервіс машинного перекладу. В середині додатку є можливість здійснювати грошові перекази та робити оплату послуг [27].

Отже можна зробити висновок що WeChat має переваги в багатофункціональності, включаючи платіжні сервіси, соціальні мережі та навіть замовлення послуг, що робить його незамінним у Китаї. На рис. 2.4 зображено приклад інтерфейсу WeChat.

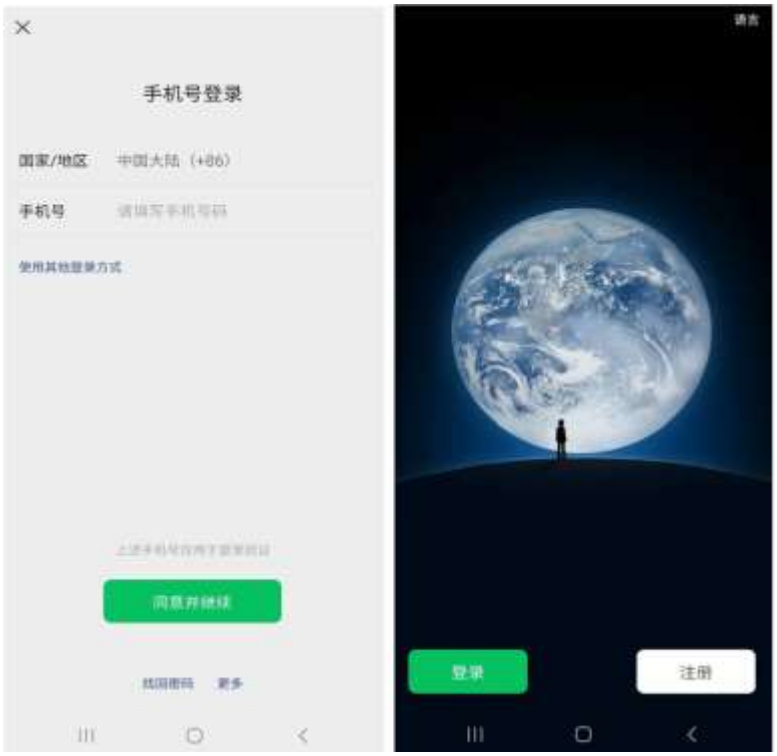

Рис 2.4 Інтерфейс WeChat

QQ – сервіс миттєвого обміну повідомленням, а також однойменна програма-клієнт, розроблена китайською компанією Tencent. Підтримується телекомунікаційною компанією Tencent. QQ пропонує послуги, такі як онлайн-ігри, музика, покупки, мікроблогінг, фільми та програмне забезпечення для групового та голосового чату [28].

Особливостями QQ є обмін повідомленнями, іграми та іншими розважальними функціями.

Wire – це месенджер, орієнтований на бізнес-користувачів, але доступний і для приватного використання. Він пропонує наскрізне шифрування для всіх типів комунікації та має відкритий вихідний код [29].

Wire дає змогу організовувати віртуальні конференції та створювати групові чати. У месенджері легко обмінюватися медіаповідомленнями та безпосередньо під час розмови створювати ескізи [30]. Додатково має функцію самознищення повідомлень, протокол Proteus для надійного шифрування, який розроблений на основі протоколу Signal. Завдяки відкритому коду має постійні аудити. На рис. 2.5 зображено приклад інтерфейсу Wire.

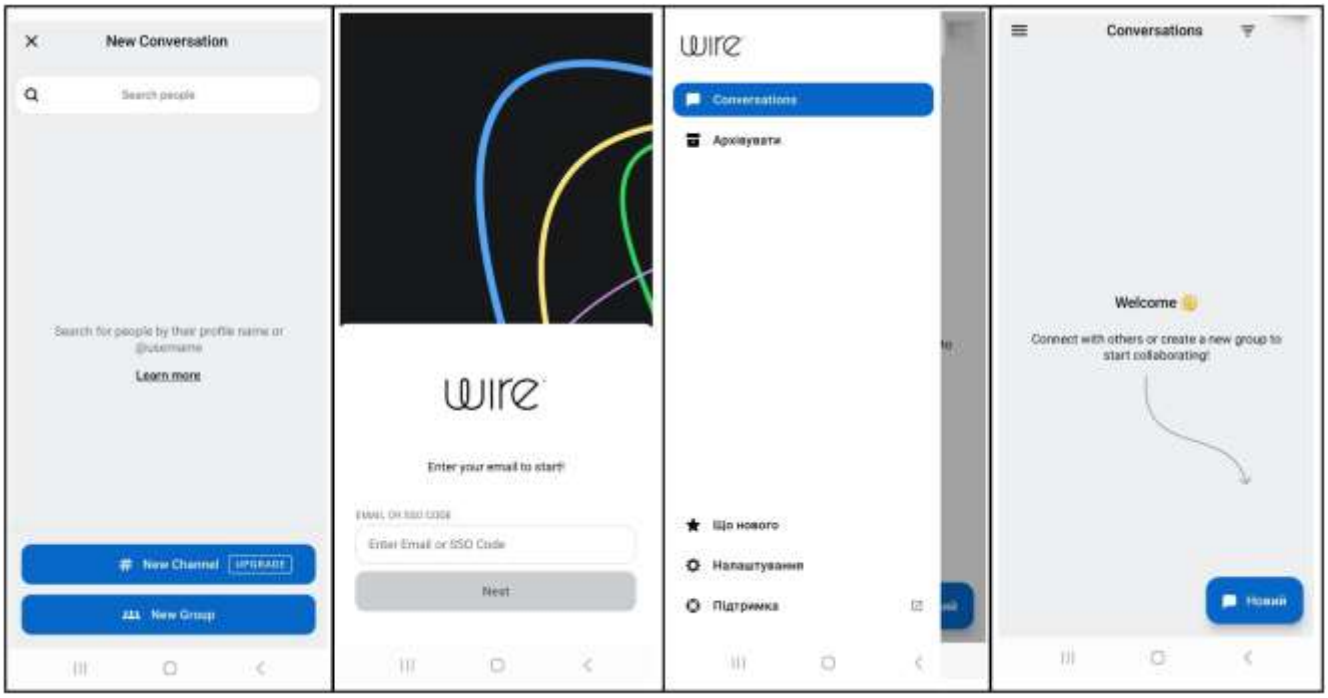

Рис. 2.5 Інтерфейс Wire

Telegram, з моменту заснування в 2013 році братами Дуровими, стрімко еволюціонував у глобального лідера серед месенджерів. За останніми даними Павла Дурова, платформа досягла вражаючого результату – 900 мільйонів активних користувачів. Фінансова оцінка Telegram у $30 мільярдів, за твердженням засновника, ставить його в ряд найдорожчих технологічних компаній світу. Компанія не зупиняється на досягнутому і розглядає можливість первинного публічного розміщення (IPO), що, безумовно, може відкрити нові горизонти для розвитку та інновацій [31].

Ключові особливості Telegram – швидкість та зручність, інтуїтивно зрозумілий інтерфейс та швидка синхронізація між пристроями. Функціональність – текстові повідомлення, голосові та відеодзвінки, групові чати до 200 000 учасників. Також є додаткові функції які мають можливість самознищення повідомлень, обмін файлами та документами. Являє собою соціальну платформу – підтримка каналів з мільйонами підписників та масштабних груп [32].

Google Messages додаток, який дозволяє обмінюватися файлами, голосовими повідомленнями, геоданими, відеодзвінками/дзвінками та текстовими повідомленнями за допомогою RCS.

Месенджер має наскрізне шифрування що покращує безпеку користування ним та більшу конфіденційність для користувачів. Завдяки RCS-технології надає можливість спілкуватися з власниками iPhone, створювати групові чати та інші цікаві функції, наприклад, бачити набір повідомлення співрозмовником. Інтеграція з ШІ дозволяє писати більш розширену думку в повідомленнях, що покращають розуміння написаного. Месенджер також має синхронізацію з іншими пристроями, що дозволяє користувачеві почати чат на телефоні, а продовжити на іншому пристрої, з дрібничок є персоналізація чатів та повідомлень. Додатково розробники додали функцію автоматичного видалення SMS повідомлень з одноразовими паролями, які можуть надсилати інші сервіси для перевірки входу.

Session – месенджер, який має високий рівень конфіденційності завдяки відсутності обов’язкової прив’язки номера телефона або електронної пошти, має наскрізне шифрування, приховує IP-адреси користувачів та не зберігає журнал активності.

Simple-X месенджер, як і Threema, не має ідентифікаторів номеру телефону або e-mail. Не має хмарного сховища, все листування зберігається виключно локально на пристрої. Наскрізне шифрування на повідомлення, відеофайли, групи, дзвінки та голосові повідомлення за замовчуванням.

Посилання на профіль можна згенерувати і відправити одноразову адресу профіля довіреним каналом – як це реалізовано у Signal. Але навіть маючи таку адресу профіля – є можливість прийняти або відхилити запит на спілкування. Наприклад, якщо ваш начебто надійний контакт поширив цю адресу із іншими людьми.

Наявність режиму «інкогніто», якщо його увімкнути, то для нових контактів, для яких ви генеруєте одноразову адресу свого профілю – буде відображатися не справжнє, а випадкове ім’я профілю та аватарка [36].

Приєднатися до групового чату можливо лише за запрошенням, знайти групу за пошуком неможливо. У групі доступні ролі користувачів, адміністраторів або власників. Можна заблокувати/розблокувати історію попередніх повідомлень у чаті для нових учасників.

Месенджер має децентралізовану система серверів: є сервери самого SimpleX, які публічні, але можна створити власний сервер, використовуючи повністю відкритий та доступний код серверної частини SimpleX. Кожен користувач SimpleX має можливість самому визначати, через які сервери отримувати чи відправляти повідомлення. Це унеможливлює атаки типу MITM [36].

На рис. 2.6 зображені популярні месенджери, які користуються популярністю в Україні у 2025 році.

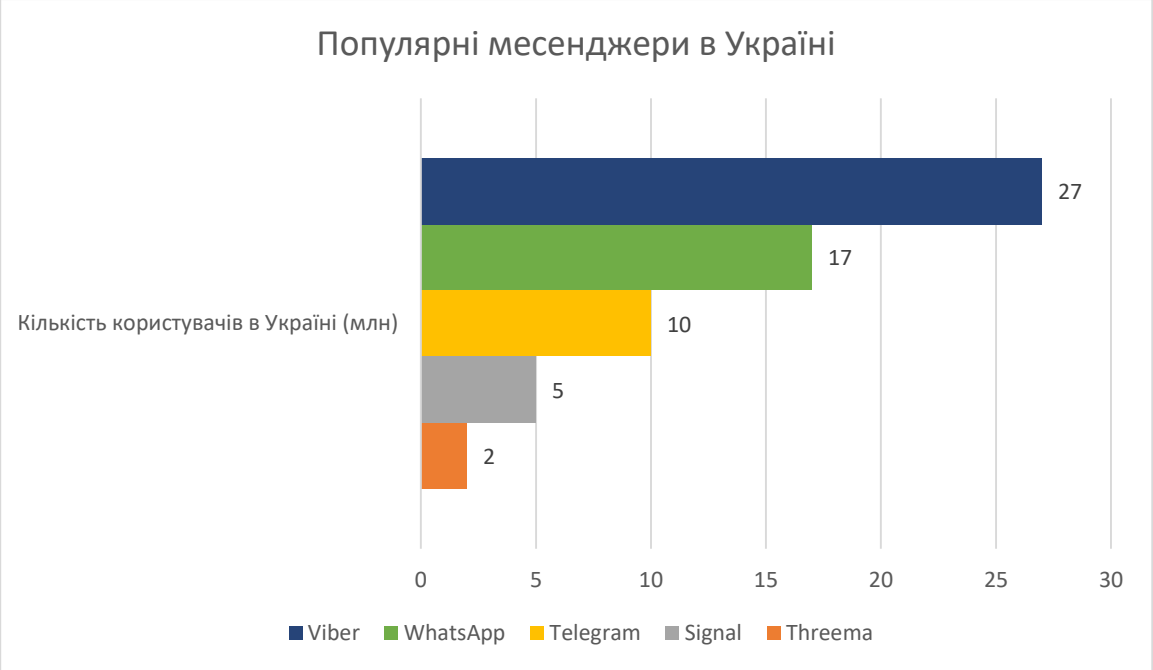

Рис. 2.6 Популярні месенджери в Україні

Viber – найбільш популярний месенджер, яким користуються більшість опитаних українців за результатом опитування КМІС [33].

VoIP-застосунок для дзвінків і обміну повідомленнями. Застосунок підв'язується до номера мобільного телефону, але не використовує мобільну мережу. Для здійснення дзвінків і обміну повідомленнями програма потребує інтернет-з'єднання. У месенджері можна створювати чат-боти, канали, спільноти та здійснювати платежі. Станом на 2025, застосунок був встановлений у 98% власників смартфонів в Україні [34].

В месенджері присутні додаткові функції для користувачів, а саме: зміна теми, різні наліпки та шрифти. Водночас додаток має наскрізне шифрування за замовчуванням і не потребує від користувача додаткового вмикання даної функції [23].

Тому можна зробити висновок, що Viber є найпопулярнішим серед користувачів в Україні завдяки простоті використання, зрозумілому інтерфейсу та легкості додавання контактів. На рис. 2.7 зображено приклад інтерфейсу Viber.

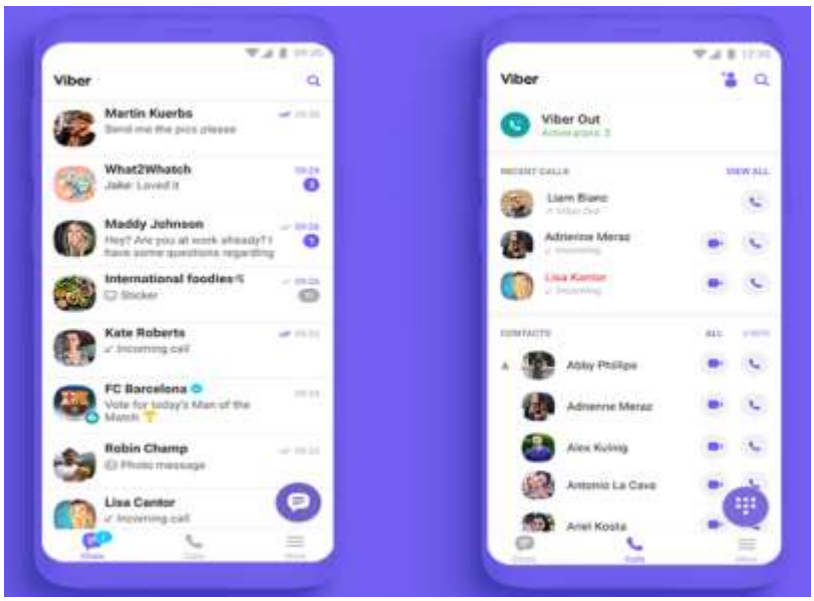

Рис. 2.7 Інтерфейс Viber

Telegram – набираючий популярність месенджер від 2022 року, став основною платформою для отримання новин. Загалом месенджером користуються понад 10 мільйонів українців.

З плюсів даного месенджера є:

висока швидкість та простота у використанні – додаток має простий та зрозумілий інтерфейс та працює навіть при поганому інтернет з'єднанні;

зручність – Telegram поєднує функції месенджера та платформи яка надає актуальні новини. Користувачі можуть вести особисті чати, групи та навіть створювати канали для важливої інформації, надсилати файли без обмежень, створювати ботів та користуватися ними, використовувати хмарне сховище [35].

На рис. 2.8 зображено приклад інтерфейсу Telegram.

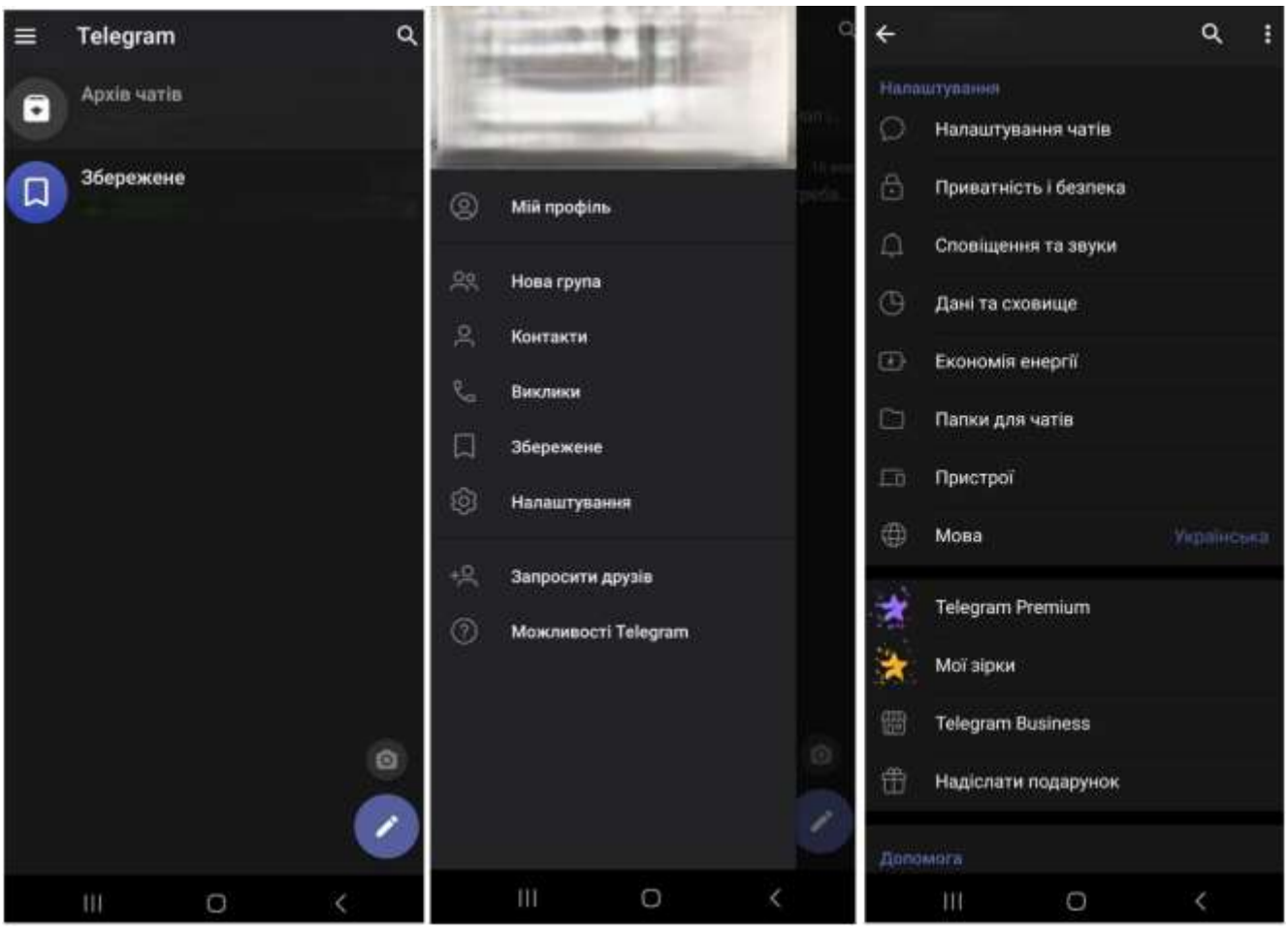

Рис. 2.8 Інтерфейс Telegram

WhatsApp – менш популярний, ніж Viber і Telegram, але все ще має стабільну аудиторію. Найчастіше WhatsApp використовують для спілкування з родичами та друзями за кордоном, оскільки він популярний у Європі та США. У сфері бізнесу WhatsApp часто застосовується для підтримки клієнтів (банки, служби доставки, інтернет-магазини).

WhatsApp має мінімалістичний інтерфейс, відсутні зайві функції та реклама. Усі чати та дзвінки в WhatsApp мають E2EE за замовчуванням, що захищає їх від прослуховування. WhatsApp дозволяє видаляти повідомлення для всіх, додатково у 2023 році додали можливість редагування повідомлень.

Signal – Заснований у 2014 році Меттом Розенфельдом, відомим криптографом та захисником цифрової приватності, Signal швидко став синонімом надійності серед месенджерів. На відміну від багатьох конкурентів, Signal – це некомерційний проєкт, що фінансується грантами та пожертвами. Це дозволяє

розробникам з Signal Foundation зосередитися на безпеці користувачів, а не на монетизації їхніх даних.

Має великі плюси в безпеці, а саме: власний протокол наскрізного шифрування, який захищає всі види комунікації, додаткові функції захисту такі як – зникаючі повідомлення, захист додатку паролем. Відкритий код, регулярні перевірки безпеки, підтримка експертів з приватності робить месенджер більш надійним та відкритим для користувачів в плані довіри [32].

Signal використовує той самий протокол шифрування, що й WhatsApp та Facebook Messenger, але належить некомерційній організації, що підвищує довіру до нього.

Threema – платний месенджер, розроблений швейцарськими підприємцями Мануелеем Каспар, Сільваном Енглер і Мартіном Блаттер. Швидко здобувши для Threema репутацію одного з найбезпечніших месенджерів. Головна філософія компанії – забезпечити максимальну приватність даних користувачів, не займаючись збором чи монетизацією їх особистої інформації.

Threema має дуже важливі для безпеки користувача плюси такі як: наскрізне шифрування для повідомлень та дзвінків, ключі шифрування зберігаються на пристроях користувачів, генерує унікальний Threema ID, що дозволяє використовувати додаток без вказівки імені, номера телефону чи e-mail, що дозволяє зберегти анонімність. З додаткових функцій, месенджер має QR-код для безпечного обміну контактами при особистій зустрічі [32].

Порівняльний аналіз безпеки месенджерів представлений в таблиці 2.1.

Таблиця 2.1

Порівняльний аналіз безпеки месенджерів

Функції	WhatsApp	Viber	Telegram	Signal	Threema
Чи ввімкненно шифрування за замовчуванням	Так, якщо пристрій підтримує	Так, якщо пристрій підтримує	Ні	Так	Так
Криптографічні примітиви	Signal Protocol, Double Ratchet, X3DH, PreKeys AES-256-CTR, Curve25519, HMAC-SHA256	AES-256, Curve25519, HMAC-SHA256, SHA-256	MTProto 2.0, AES-256-IGE, SHA-256, RSA-2048, Diffie-Hellman	Signal Protocol, Double Ratchet, X3DH, PreKeys AES-256, Curve25519, HMAC-SHA256	NaCl, Curve25519, Xsalsa20, Poly1305, SHA-256
Чи забезпечує месенджер конфіденцій-ність передачі даних	Так	Так	Ні	Так	Так
Чи шифруються метадані	Ні	Ні	Ні	Так	Так
Чи надає компанія звіт про прозорість	Ні	Ні	Ні	Так	Так
Чи проводився незалежний аудит коду та аналіз безпеки	Так (2022-2023)	Ні	Так (2020)	Так (2022)	Так (2022)
Чи присутня анонімна реєстрація	Ні	Ні	Ні	Ні	Так
Чи присутня у месенджері двофакторна автентифікація	Так	Ні	Так	Ні	Так

Серед, здавалося б, великої кількості месенджерів, їх різному функціоналу та можливостям, лише декілька є достатньо захищенними аби ними могли безпечно користуватися державні установи та структури. В Україні, коли безпека та швидка комунікація має стратегічне значення, загальнодержавною проблемою є

забезпечення державних установ, МО України та організації критичної інфраструктури захищеним месенджером вітчизняної розробки (ЗМВР).

Зараз месенджери Signal та WhatsApp стали важливими інструментами, як для внутрішньої взаємодії, так і для зовнішніх контактів. Signal зазвичай використовується для обміну конфіденційною інформацією між працівниками державних органів, тоді як WhatsApp частіше застосовується для організаційних питань, координації дій у кризових ситуаціях або комунікації з громадськістю.

Signal вирізняється своїм акцентом на приватність і безпеку. Цей месенджер розроблений некомерційною організацією, а його вихідний код є повністю відкритим. Це означає, що незалежні експерти можуть перевірити відсутність шпигунських модулів або вразливостей у системі. Signal використовує свій протокол шифрування – Signal Protocol, який є найнадійнішим протоколом у світі на поточний час, протокол забезпечує наскрізне шифрування всіх повідомлень, дзвінків та переданих файлів. Навіть сервери месенджеру не мають доступу до змісту листування. Уся інформація зберігається лише на пристрої користувача, а після видалення або доставки повідомлення вони не залишають жодного сліду на сервері. Signal також не збирає метадані, не зберігає списки контактів і не відстежує активність користувачів. Усе це робить його одним із найзахищеніших способів зв’язку, який активно рекомендують експерти з кібербезпеки та правозахисні організації. Месенджер не має реклами, не аналізує поведінку користувачів і не має комерційного інтересу у зборі даних. Завдяки цьому державні службовці можуть бути впевнені, що їхні розмови залишаються повністю приватними, що особливо важливо під час службових перемовин або обміну оперативною інформацією.

WhatsApp, у свою чергу, хоч і належить корпорації Meta, також має високий рівень захисту завдяки використанню того ж протоколу Signal Protocol. Усі повідомлення, дзвінки та передані файли зашифровані й доступні лише відправнику та отримувачу. Проте на відміну від Signal, WhatsApp зберігає певні метадані, а саме: номери телефонів, дати активності чи інформацію про зв’язки

між користувачами. Незважаючи на це, WhatsApp популярний серед військових та став майже універсальним засобом спілкування, що дозволяє швидко координувати дії не лише всередині державних структур, а й між ними та громадськістю. Це особливо важливо під час надзвичайних ситуацій, гуманітарних операцій або комунікації з місцевими адміністраціями. Його популярність пояснюється можливістю створення групових чатів до тисячі осіб, передачу великих файлів, геолокації, голосові та відеодзвінки.

У державній практиці WhatsApp часто використовується там, де необхідна оперативність і доступність, а Signal – там, де критично важлива безпека. Таким чином, українські служби комбінують обидва інструменти: Signal забезпечує максимальний рівень конфіденційності та довіри між співробітниками, а WhatsApp дозволяє підтримувати широку комунікацію з великою кількістю людей у найкоротші терміни. Ця гнучкість у виборі каналів зв'язку дозволяє державним органам одночасно залишатися ефективними та захищеними в умовах постійних кіберзагроз і гібридних викликів із якими сьогодні стискається Україна.

2.1.2 Проблеми та загрози безпеці месенджерів на мобільних пристроях

Немає додатків, які мають стовідсотковий захист і навіть при оновленнях та спробах вдосконалити месенджери розробник навмисно або ні залишає прогалини в захисті системи. Розглянемо детальніше проблеми месенджерів та до чого вони можуть привести.

Facebook Messenger – один з найпопулярніших месенджерів, але основна проблема даного месенджера – це відсутність наскрізного шифрування (E2EE) за замовчуванням. Через це чати не захищенні від перегляду сервером Meta. Компанія не розповідає про свої функції, тому більшість користувачів не знають про спеціальний режим "Secret Conversation" що забезпечує E2EE.

Meta, яка є сервером для даного месенджера, офіційно заявляє, що не збирає данні користувачів, їх повідомлення не скануються для реклами, метадані (час, адреса) не зберігаються і не передаються правоохоронним органам за запитом. Попри заяви код месенджера закритий і жодних належних аудитів безпеки не

проводиться тому користувачам доводиться повністю покладатися лише на слова Meta, яка неодноразово мала проблеми з витоком, викраденням та зламом їх серверів, що дозволяло викрадати та продавати дані користувачів.

Як висновок, Facebook Messenger не надійний через втрату даних, недотримання конфіденційності в чатах через злам або закон країни, збір даних для детального досьє на користувача, що може бути використано у комерційних або політичних цілях.

Viber – популярний серед українців месенджер, який має E2EE у приватних чатах, але має проблеми з прозорістю коду та публічними аудитами (код програми закритий, аудитів не проводить), тому ще один додаток, який потребує довіри на слові. Ще одна з проблем – це резервне збереження копій. Якщо копії зберігаються у хмарі iCloud чи Google, то вони можуть бути незашифровані, через це можливий доступ до історії чату без злому пристрою.

Компанія має доступ до низки інформації про користувачів і зберігає її в незашифрованому вигляді, наприклад, контакти користувача, які підтягуються з телефонної книги, тому при помилці працівників або через кіберінцидент можливий виток даних і без зламу користувача.

З цього випливає, що користування Viber несе ризик втрати приватних контактів та листування з ними, можливі потенційні фішингові атаки через витік даних, а також має слабкий захист у хмарі.

Telegram – проблемний для українців месенджер через його засновника, який є росіянином і хоч засновник розповідає про свою лояльність до росії, користувачам знову треба вірити на слово. В телеграмі існує дуже багато каналів та чатів, які виправдовують агресію росії проти України та підтримують/спонукають до геноциду українців, поширюють фейки та вводять в оману користувачів месенджера. Засновник та працівники не займаються блокуванням таких чатів та не слідкують за контентом, який присутній в таких чатах.

Багато користувачів вірять, що їх дані захищені E2EE тому, що про це стверджують самі розробники, однак цей захист не вмикається автоматично та доступний лише для особистих діалогів. Групові чати, канали не мають даного захисту. Вони зберігаються у хмарі месенджера разом з ключами розшифрування, що дозволяє компанії отримати доступ до листування.

Слід зауважити що Telegram використовує власний криптографічний протокол MTProto, який у професійному середовищі вважається ненадійним, як, наприклад, стандарт Signal Protocol, який вважається більш надійним. Саме через це криптографи висловлюють сумніви до коректності та стійкості протоколу MTProto.

Telegram має широкий функціонал, але поступається в питаннях безпеки. Його часто використовують для фішингових атак та крадіжки акаунтів. В оцінці експертів, серед негативних згадувань щодо безпеки Telegram займає перше місце [23].

Наслідки користування Telegram є достатньо критичні та негативні для користувача через відсутність захисту всіх чатів, сумнівний криптографічний протокол, який може бути вразливішим за існуючі, ризик на втручання та моніторинг даних державою, ворогом або продажем даних третім країнам.

WhatsApp месенджер, який вмикає E2EE за замовчуванням для всіх чатів. Проблемою є те, що Meta збирає і зберігає інформацію про те, з ким, коли та, як часто користувачі спілкуються між собою, данні, які збираються не зашифровані та використовуються для маркетингованих компаній та правоохоронних органів, іноді цього достатньо аби робити висновки про життя користувача. Месенджер також не дозволяє повністю відмовитися від прив’язки до номера телефону [23].

Резервні копії теж під питанням захисту бо вони зберігаються в хмарі ICloud або на Google Drive і можуть бути незашифровані чи шифруватися з ключем доступу, що дозволяє зловмиснику зламати хмару та отримати доступ до всієї історій повідомлення.

В історії месенджера були прямі вразливості (Pegasus атака) – шпигунське ПЗ, яке можна було встановити на телефон через пропущений виклик у WhatsApp.

Отже небезпека користування WhatsApp полягає в детальному моніторингу метаданих компанією, передача даних рекламодавцям, можливий продаж даних, небезпека витоку резервних копій, залежність від репутації та політики Meta.

SimpleX, як і Telegram, створений командою, де присутні росіяни, що не може не напружувати користувачів з України. Немає хмарного сховища, тому неможливо синхронізувати свій профіль на різних пристроях. Але можна зі смартфона транслювати свій профіль на комп'ютер чи лептоп, через сканування QR-коду, як це працює у WhatsApp.

Якщо забули пароль та пін-код до SimpleX Chat на своєму пристрої, то відновити локальний контейнер з базою даних на пристрої буде неможливо. Щоб перенести все листування у SimpleX на новий пристрій, потрібно на старому пристрої «зупинити» месенджер, скачати локальну базу даних і потім експортувати архів на новий пристрій, це може зробити досвідчений користувач, але новачку буде складно, що є недоліком, який більше відноситься до незручності [36].

Google Messages – месенджер, який має новий стандарт RCS, що замінює SMS/MMS. Так само зберігає та збирає метадані користувачів та зберігає у відкритому вигляді, що дозволяють дізнатися місце перебування, дізнатися про активність та особисті звички користувачів. Відсутність прозорості у криптографії, код сервісу закритий, що унеможливлює перевірки сторонніх експертів на наявність критичних помилок або механічних збоїв.

Дані Google Messages не завжди шифруються одразу на пристрої через це є шанс викрадення повідомлень через зараження шпигунським ПЗ або викрадення телефона.

Ще одною з проблем є шахрайські RCS повідомлення. Шахрай надсилає фейкове повідомлення, яке нічим не відрізняється від звичайного повідомлення. Через це користувач може легко потрапити на фішинг.

Викрадення даних, можливі шахрайства та маніпуляції користувачами, втручання в життя користувача шляхом збирання метаданих робить Google Messages ненадійним.

Signal – месенджер, який рекомендується використовувати державникам та військовим під час війни, журналістам та правозахисникам, але, із певними застереженнями, підтримує функції редагування, видалення повідомлень та їхнє самознищення через таймер, обмеження скриншотів і налаштування приватності профілю. Месенджер доступний на Android, iOS, Windows, MasOS і Linux [23]. Додаток хоч і відомий високим рівнем захисту та відкритістю, користувач все одно залежний від прив'язування до телефону. Сервер Signal не зберігає хмарні копії листування на сервері через це, якщо втрачається носій даних то втрачається і листування. Групові виклики можливі лише між учасниками одного чату, якщо всі використовують найновішу версію застосунку; обмеження – до 50 осіб [23].

WeChat став важливим інструментом для українців, які мають справи з Китаєм, будь то бізнес, освіта чи культурні зв'язки. Українські компанії можуть використовувати WeChat для встановлення контактів з китайськими партнерами, проведення переговорів та укладання угод. Це зручно для експортерів, імпортерів та підприємців, які працюють на китайському ринку. Студенти, дослідники та викладачі можуть використовувати WeChat для зв'язку з китайськими університетами та освітніми програмами [37].

Мінусом месенджера є відсутність наскрізного шифрування та державний нагляд Китаю. Користувачі WeChat з Китаю знаходяться під важким державним наглядом, це означає, що уряд цензурує контент та активність у додатку. Все, що публікується з Китаю, піддається спостереженню, і китайський уряд може видаляти все, з чим не погоджується [38]. Месенджер має обмежені функції

редагування і видалення повідомлень – тільки в перші хвилини після надсилання; відсутня підтримка повного самознищення повідомлень [23].

Користувачі, які перебувають на території Китаю мають обмежений вибір серед месенджерів оскільки більшість месенджерів, якими користуються в світі, заблоковані:

- WhatsApp заблокований ще з 2017 року, а у 2024-му Apple прибрала його з китайського App Store за наказом уряду КНР.;
- Telegram заблокований з 2015 року;
- Signal заборонений з 2021 року, а у 2024 його прибрали з App Store;
- Facebook Messenger заборонений разом з Facebook з 2009 року;
- Viber заблокований з 2014 року;
- Snapchat перебуває під забороною з 2010 року [23].

QQ, як і WeChat має китайське походження, а це означає, що додаток теж контролюється китайськими службами, немає наскрізного шифрування, блокування контенту, з яким не погоджується китайська влада. Додатково месенджер має слабку підтримку іноземних користувачів і реєстрація потребує наявності китайського номера телефону.

Wire, Session, Threema мають надійний захист, але не сильно популярні, через це можуть бути складноші знайти співбесідника. Ці месенджери більш підходять, якщо користувач має друзів, члена родини, знайомого в цих месенджерах для спілкування. Додатково Threema серед трьох платний, що додатково впливає на кількість користувачів. Session має децентралізовану мережу, через що повідомлення надходять довше або взагалі не дійдуть до співрозмовника. Wire відштовхнула частину користувачів, коли змінила юрисдикцію і зареєструвалася у США, тим самим поставила під сумнів свою повну незалежність [37]. Порівняльний аналіз популярних месенджерів представлено в додатку А.

2.2 Порівняльний аналіз методів забезпечення безпеки сучасних месенджерів

Все частіше користувачі будь-якого продукту хочуть знати, наскільки він безпечний в користуванні та які методи захисту конфіденційності та приватності присутні в продукті, яким вони користуються. Через це розробники сучасних месенджерів впроваджують широкий спектр методів захисту даних, які мають відповідати стандартам безпеки, таким як ISO/IEC 27001, GDPR, HIPAA, NIST SP 800-63, TLS 1.3 та інші.

2.2.1 Шифрування повідомлень

На даний момент один з найефективніших механізмів захисту, які використовуються є наскрізне шифрування (E2EE). Метод передбачає, що повідомлення шифрується безпосередньо на пристрої відправника і розшифровується лише на пристрої отримувача. Завдяки такому методу дані перебувають у зашифрованому вигляді, що робить їх абсолютно недоступними навіть для серверу, через який проходить трафік і він не має технічної можливості прочитати вміст повідомлення, оскільки не володіє ключами шифрування. Міжнародні стандарти, як, наприклад, AES-256 для систематичного шифрування та алгоритм обміну ключами Diffie-Hellman або алгоритм Double Ratchet, забезпечують високу стійкість до атак. Серед месенджерів, що використовують E2EE за замовчуванням, можна назвати Signal, Thremma, WhatsApp. Хоча метод і має максимальний захист від перехоплення та стороннього доступу, але ускладнює реалізацій деяких функцій, наприклад, відновлення повідомлень після втрати пристрою. Схема наскрізного шифрування зображена на рис. 2.9.

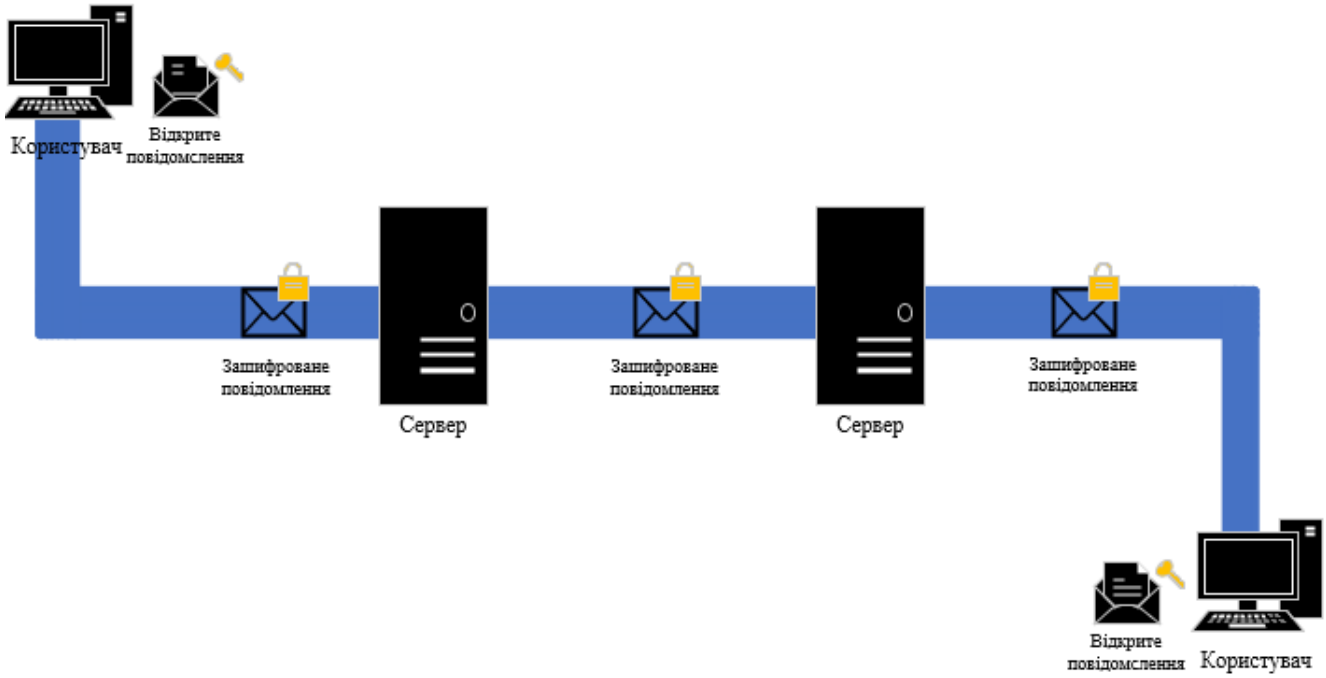

Рис. 2.9 Схема наскрізного шифрування

Наступний поширений підхід – це транспортне шифрування. Даний тип шифрування захищає дані лише під час їх передавання мережею, в більшості за допомогою TLS або його попередника SSL. Даний вид шифрування надає серверу доступ до розшифрованого вмісту повідомлень, оскільки сервер є проміжною точкою, яка отримує дані у відкритому вигляді після завершення передачі повідомлення. Такий підхід використовується в Facebook Messenger або у стандартних чатах Telegram. Метод захищає від пасивного перехоплення, наприклад, від атаки «людина посередині» (MITM), але не гарантує конфіденційності перед самим сервісом або у випадку зламу серверів.

Окрім цього, у месенджерах застосовується локальне шифрування, воно спрямоване на захист даних, що зберігаються безпосередньо на пристрої користувача. У цьому випадку повідомлення або їхня база шифруються і доступ до них можливий лише після введення пароля, PIN-коду або біометрії. Даний метод не захищає під час передачі даних, але дозволяє захистити дані, якщо телефон викрадуть чи загублять. Прикладом реалізації такого шифрування є Signal, або Telegram, який пропонує додатково встановити пароль для входу в додаток.

Деякі месенджери поєднують кілька підходів і утворюють гібридні моделі шифрування. Це допомагає знаходити баланс між безпекою та функціональністю. Прикладом є WhatsApp, він використовує E2EE для повідомлень, але передає метадані через TLS. Threema забезпечує E2EE, зберігаючи ключі шифрування лише на пристроях та додатково шифрує локальні копії повідомлень. Такі гібридні рішення роблять месенджер стійкішим до перехоплення трафіку та додають захист до фізичного доступу.

Також не можна забувати про протоколи шифрування безпеки. Серед найбільш відомих є Signal Protocol, який застосовується у Signal, WhatsApp та у режимі секретних чатів Facebook Messeger. Він базується на комбінації алгоритму Double Ratchet, протоколу Diffie-Hellman та використанні PreKeys для забезпечення асинхронної передачі. Протокол MTProto, створений спеціально для Telegram, застосовує власну криптографічну схему, яка поєднує симетричне та асиметричне шифрування. Протокол визначає 3 рівні: високорівневий шар, визначений взаємодія програми з API, криптографічний шар та компонент доставки, відповідальний за вибір способу передачі повідомлень (транспортного протоколу) [23].

Шифрування повідомлень здійснюється за схемою, що зображена на рис.2.10 (темним відмічені секретні параметри шифрування).

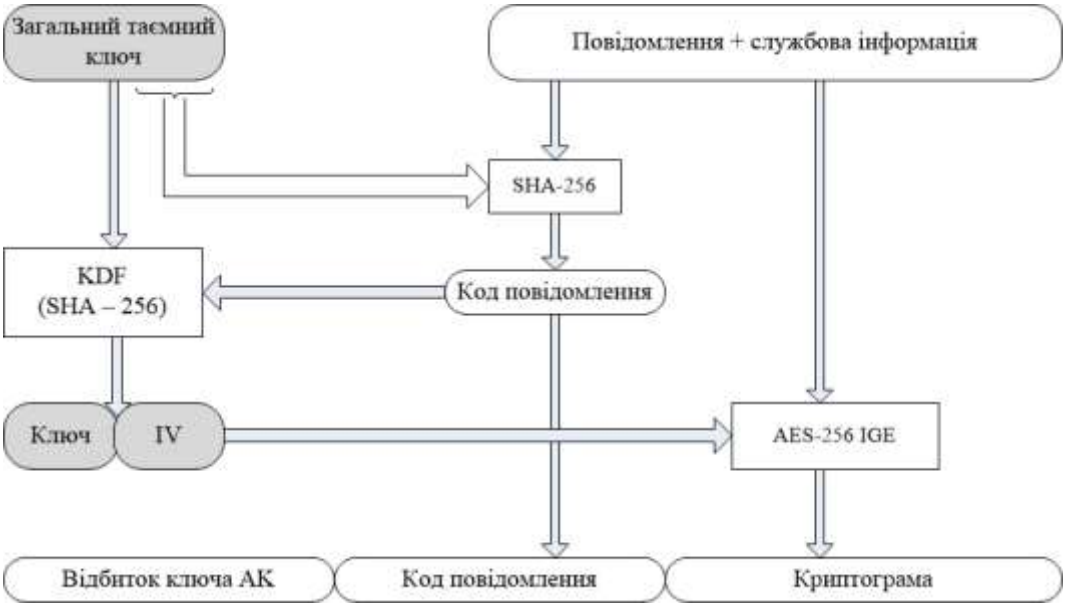

Рис. 2.10 Схема шифрування повідомлень MTProto

2.2.2 Аутентифікація та авторизація користувачів

Аутентифікація – процес перевірки достовірності особи користувача, який намагається отримати доступ до сервісу. Авторизація – визначення прав та привілеїв користувача після успішної аутентифікації.

Процедура аутентифікації в месенджерах залежить від обраної моделі безпеки та технічних особливостей сервісу. Традиційним і найпоширенішим методом є аутентифікація за допомогою пароля або PIN-коду. Цей вид є двофаткорною аутентифікацією (2FA), вона передбачає підтвердження особи за допомогою двох незалежних факторів: щось, що користувач знає, наприклад, пароль або PIN-код та щось, що користувач має – мобільний телефон, одноразовий код з додатку. Для даного елементу захисту викладено рекомендації у стандарті NIST SP 800-63B. Стандарт визначає вимоги до складності паролів, алгоритмів генерацій кодів і механізмів багатофакторного входу. Хоч цей метод досі використовують, його намагаються замінити або доповнити на більш безпечні механізми, наприклад, месенджери почали все частіше використовувати одноразові коди підтвердження, що надсилаються на пошту або через SMS, якби користувач мав змогу зайти або авторизуватися. Метод спрощує користування месенджерами в мобільному середовищі і користувачу не потрібно згадувати свій пароль від додатка.

Також в месенджерах присутня багатофакторна аутентифікація (MFA), принцип її роботи зображений на рис. 2.11, вона відрізняється від двофакторної тим, що має більше поєднань для входу в месенджер. Наприклад Signal або Telegram можуть використовувати поєднання одноразового коду з паролем або біометрією.

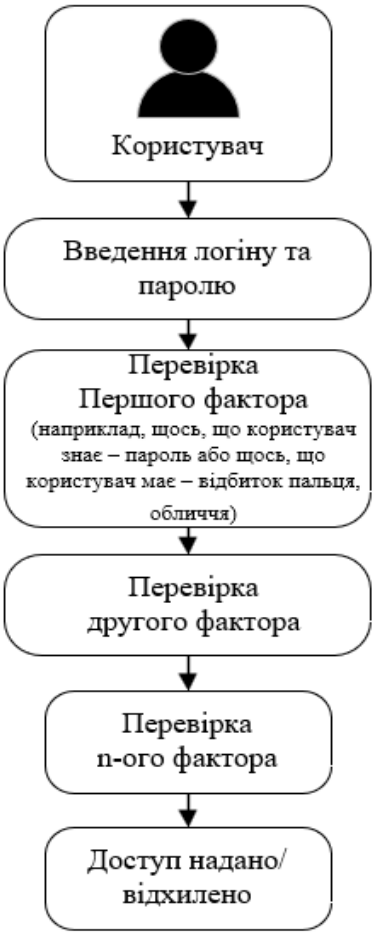

Рис. 2.11 Принцип роботи MFA

Біометрична аутентифікація, що базується на відбитках пальців, розпізнаванні обличчя чи скануванні ока, є зручною для користувачів і водночас підвищує захист від несанкціонованого доступу. Біометрія зберігається на пристрої, а не в месенджері, що знижує ризик втрати біометричних даних.

Ще один з методів аутенфікації – це зовнішні сервіси або єдині облікові записи. Наприклад, у деякі месенджери можна увійти або зареєструватися за допомогою Google або Apple ID. Такий підхід спрощує процес реєстрації, але створює залежність від сторонніх компаній та підвищує значимість їх механізмів безпеки.

У месенджерах, орієнтовних на підвищену конфіденційність, наприклад, Threema, аутентифікація в месенджері відбувається без прив’язки до номера телефона чи електронної пошти. Користувач отримує унікальний ідентифікатор, а

обмін ключами шифрування відбувається автоматично під час першого контакту. Такий підхід дозволяє залишатися анонімним та зберігати безпеку комунікації.

Авторизація у месенджерах тісно пов’язана з внутрішньою логікою роботи сервісу та його функціоналом. У більшості випадків після аутентифікації користувач отримує повний доступ до функціоналу месенджера. Однак, в окремих випадках авторизація може визначати додаткові функції. Наприклад, у групових чатах Telegram, авторизація впливає на додаткові функції групи такі, як зміна назви групи, керування дозволами користувачів групи, їх видалення або додавання.

Однак, навіть найсучасніші методи захисту при авторизації та аутентифікації не гарантують абсолютної безпеки, якщо користувач нехтує базовими правилами кібергігієни. Використання простих паролів, відсутність додаткового захисту (2FA, MFA або біометрія), завантаження месенджера не з офіційного джерела чи надавання облікового запису іншим особам може мати наслідки та втрачені дані. Через це більшість розробників вдосконалюють безпеку месенджерів, пов’язану з персональними даними, та активними сеансами.

2.2.3 Захист від вірусів та шкідливих програм

Найпоширенішим зараженням через месенджери є розсилання заражених файлів. Це можуть бути архіви з вбудованим виконуваними файлами під виглядом документів або зображень, медіафайли, що містять експлойти. Зловмисники можуть використовувати компроментовані облікові записи реальних користувачів, щоб надіслати подібний файл їхнім контактам, адже повідомлення від знайомої людини викликає менше підозри.

Сучасні віруси та шкідливі програми, що поширюються через месенджери, можуть мати різну мету та функціонал. Деякі спрямовані на крадіжку облікових даних, паролів чи токенів доступу, а інші спрямовані на шифрування файлів з подальшим вимаганням викупу. Існують також шпигунські програми, які здатні перехоплювати повідомлення, знімки, аудіо та відео з пристрою з метою видалення, модифікації та шантажу.

Для протидії загрозам, пов’язаним з вірусами та шкідливими програмами, у месенджерах, важливо поєднувати технологічні засоби та обачність користувача. На рівні додатків розробники впроваджують вбудовані механізми фільтрації шкідливого контенту, сканування файлів перед завантаженням, автоматичне блокування підозрілих посилань. Деякі месенджери застосовують системи машинного навчання та аналізу вмісту та поведінки облікових записів, що дозволяє швидше виявити зловмисників.

З точки зору користувача, ключовим елементом захисту є обачність, обізнаний користувач знає, що не варто відкривати підозрілі посилання, файли, які відправлені від невідомих користувачів. У разі отримання підозрілого файлу користувач може перевірити файл в онлайн-сервісах або через локальний антивірус перед відкриттям.

Загалом інтеграція антивірусних рішень у месенджери – поширена практика в корпоративному середовищі. У бізнес версії WeChat система сканує усі отримані файли на наявність шкідливого коду ще до того, як користувач їх відкриє. Завдяки цьому знижується ризик зараження пристрою, що особливо актуально для організацій, які працюють з конфіденційною інформацією.

2.2.4 Аналіз та блокування загроз у режимі реального часу

Одна з найпопулярніших та небезпечних загроз є фішинг та соціальна інженерія. Атака працює наступним чином – користувач отримує посилання, повідомлення або файл від зловмисника, який видає себе за знайомий контакт або сервіс, яким користується жертва, такі дії призначені для викрадення паролів чи облікових даних з метою продажу або заволодіння. В більшості атаки спрямовані на отримання SMS-кодів або кодів автентифікації для доступу акаунтів месенджерів. Для блокування такого роду повідомлень у реальному часі застосовуються системи перевірки URL-адрес, система порівнює адреси з базами відомих фішингових ресурсів, перевіряє алгоритми поведінкового аналізу, що виявляють підозрілі шаблони повідомлень, і, якщо повідомлення підпадає під підозру, то автоматично блокуються перед доставкою користувачу. Сучасні

алгоритми сучасного навчання дозволяють розпізнавати нові фішингові сторінки і додавати їх в базу, навіть якщо ці атаки не схожі за попередні та не містять очевидних помилок чи підозрілих елементів.

Наступною, не менш небезпечною загрозою є перехоплення облікових даних та має назву account takeover. Метод можливий, якщо зловмисник домовляється з оператором або підробляє документи, щоб перенести номер жертви на свою SIM-карту, це дозволяє отримувати SMS-коди відновлення паролю. Додатково зловмисник може скомпрометувати поштову скриньку або хмарні акаунти. Якщо зловмисник отримує контроль над обліковим записом або номером телефону, який в свою чергу пов’язаний з месенджером, то фактично він отримує доступ до всіх листувань та перехоплює весь акаунт жертви. Можливий і інший сценарій, оператори мобільного зв’язку мають право за собою надавати використані номери телефонів іншим користувачам при умові, що попередні не сплачували тарифний план або довго не користувались номером, через це є ризик, що месенджери, які прив’язані до телефону, можуть містити листування, дані попереднього користувача. У будь якому випадку в реальному часі системи безпеки аналізують географію спроб входу, пристрої, які намагаються виконати вхід і можуть заблокувати підозрілий логін або відправити push-повідомлення власнику акаунту про підозрілий вхід. Важливу роль тут відіграє двофакторна аутентифікація, саме завдяки їй можна ускладнити захоплення та втрату акаунту у випадку втрати, викрадення чи компрометації SIM-карти.

Серйозною загрозою конфіденційності даних можуть стати публічні Wi-Fi мережі. Саме через них зловмисник може організувати атаку MITM (людина посередині) і спробувати перехопити незашифрований трафік. Хоча більшість месенджерів захищені наскрізним шифрування, деякі мають недопрацювання та вразливості, наприклад, Telegram не має захисту E2EE у звичайних чатах, через це є вразливим. Якщо вже говорити про перехоплення, то сюди можна віднести ще один вид атаки – IMSI-catcher. Метод базується на створені фальшивих базових станцій, які дозволяють перехоплювати SMS-повідомлення та дзвінки. Для виявлення подібних загроз використовуються криптографічні механізми

перевірки ключів, хмарні сервіси та перевірки сертифікатів, а також мобільні інструменти аналізу мережевих підключень.

Атаки на біометрію та блокування екрана теж поширений метод обходу захисту. Якщо телефон захищений простим PIN-кодом або відбитком пальцю, який можна підробити або змусити користувача розблокувати пристрій, то зловмисник отримає прямий доступ до месенджерів та листування. У реальних умовах часто підглядають пароль та викрадають або примушують віддати пристрій. В таких випадках краще ставити додатковий захист на додатки, мати інший PIN-код для входу в месенджер. Саме додатковою аутентифікацією система може захистити інформацію користувача навіть під час втрати носія даних.

Додаткове джерело ризику є резервні копії в хмарі. Більшість месенджерів автоматично зберігають інформацію в хмарах Goggle Drive або iCloud. Якщо вони не зашифровані власним ключем користувача, то зловмисник зможе отримати доступ до даних, зламавши хмарний акаунт. В цьому випадку наскрізне шифрування не рятує і історію повідомлень можна буде переглянути з резервної копії. Системи захисту можуть попереджати користувача про ризики незахищених копій і пропонувати виправлення вразливості. Наприклад, WhatsApp в такому випадку пропонує увімкнути опцію E2EE backups.

Зловживання дозволів додатків теж несе загрозу конфіденційності та даним. Шкідливі програми маскуються під легітимні утиліти та отримують доступ до мікрофона, камери та файлової системи. Прикладом є трояни з правами, що дозволяють зчитувати текст з екрана і таким чином отримувати доступ до листування, на такий вид загрози не може повпливати шифрування. Сучасні операційні системи показують індикатори, якщо використовується камера або мікрофон, дозволяють обмежити доступ додатка лише на час його використання і повідомляють користувача про підозрілу активність додатка.

Окрім наведених засобів захисту від атак у реальному часі, є додаткові, окремі види захисту.

Однорангове спілкування (peer-to-peer, P2P) – один з компонентів підвищення безпеки хоча його використання обмежене специфікою мережевих інфраструктур. P2P-комунікація дозволяє передавати повідомлення напряму між пристроями користувачів без проходження через центральний сервер, це знижує ризик зламу та заволодіння файлами або повідомленнями. Такий метод безпеки дозволяє обмінюватися повідомленнями навіть в умовах відсутності інтернету за рахунок використання локальної мережі або Bluetooth.

Автоматичне стирання повідомлень – механізм, який підвищує рівень конфіденційності. Функція дозволяє налаштувати таймер, після закінчення якого повідомлення незворотньо видаляються з пристроїв користувачів. В месенджерах Telegram (функція Telegram Secret Chats) та Signal реалізовано налаштування, які дозволяють видаляти повідомлення через певний час у обох користувачів, що відповідає принципам мінімізації даних, закріпленим у GDPR. Важлива функція для обміну конфіденційними відомостями, які не повинні зберігатися тривалий час.

Захист медіа та транзакцій – ще один з критичних аспектів безпеки. У месенджерах, які підтримують передачу голосових повідомлень, файлів, відеозв'язку або фінансових операцій, шифрування поширюються не лише на текст, але й на весь мультимедійний контент. Використання TLS 1.3 для медіа забезпечує цілісність та конфіденційність передачі даних. У випадку з фінансовими переказами, які присутні у WhatsApp (WhatsApp Pay) або WeChat (WeChat Pay), застосовуються стандарти захисту, наприклад, PCI DSS.

Гнучкі способи реєстрації користувачів також сприяють підвищенню безпеки й конфіденційності. Месенджер Threema дозволяє створити запис без прив'язки до номера телефону або електронної пошти, використовуючи випадково згенерований ідентифікатор. Цей принцип зменшує кількість персональних даних, що зберігаються у сервісі.

Закриті мережі дозволяють обмежити використання месенджера лише для певного кола користувачів. Часто це використовується в компаніях для

співробітників, аби не було несанкціонованого доступу та викрадення конфіденційної інформації. Таке рішення часто відповідає стандартам безпеки ISO/IEC 27001 і передбачає повний контроль над обліковими записами, журналами активності та налаштуваннями політик безпеки.

Відповідність нормативним вимогам є критичною умовою для месенджерів, які використовуються у сферах здоров'я, фінансів або державного управління. У Європейському союзі застосовується GDPR, що регламентує обробку персональних даних, в США для медичних сервісів діє HIPPA. Месенджери, які використовуються у цих сферах, повинні гарантувати шифрування даних, контроль доступу, аудит дій користувачів та збереження журналів відповідно до вимог стандартів.

Відкритий вихідний код месенджера, наприклад, як у Signal, дає можливість незалежним експертам проводити аудит безпеки та переконуватися у відсутності вразливостей. Таке рішення підвищує довіру користувачів до месенджера, але має ризи появи шкідливих копій месенджеру з метою викрадення даних користувачів.

Існують додаткові механізми, як-от запобігання зйомці екрана, мінімізація даних при реєстрації, суворі політики зберігання даних і регулярне оновлення протоколів безпеки доповнюють загальну систему захисту. Постійні оновлення алгоритмів шифрування, що відповідають сучасним рекомендаціям NIST та IETF, дозволяють залишатися на крок попереду потенційних зловмисників.

Висновки до другого розділу

У другому розділі роботи, провівши аналіз сучасних месенджерів, я визначив перелік основних показників безпеки ЗМВР:

1. Наскрізне шифрування за замовчуванням;
2. Відкритий код – для можливості незалежного аудиту;
3. Анонімність – використання ЗМВР без прив'язки до номера телефону.
4. Збір метаданих – щоб ЗМВР не збирав надмірну інформацію про контакти, місцезнаходження тощо;

5. Автоматичне видалення повідомлень – дозвіл повідомленням зникати через певний час;
6. Двофакторна автентифікація – захищає від несанкціонованого доступу, навіть якщо пароль скомпрометовано;
7. Захист резервних копій

Отже, розробник, який прагне створити безпечний ЗМВР, має не лише враховувати правові аспекти діяльності, визначені законодавством України, але й інтегрувати сучасні технології захисту інформації, які відповідають міжнародним стандартам безпеки. На основі аналізу існуючих рішень та їхніх вразливостей необхідно сформувати чіткі вимоги до архітектури, функціоналу та рівню захисту майбутнього ЗМВР. Розробку ЗМВР можна створити з використанням міжнародного стандарту OWASP, який регулює питання створення мобільних додатків (див. розділ 3).

РОЗДІЛ 3

ФОРМУВАННЯ ВИМОГ ДО ПРОЄКТУВАННЯ ТА ПОБУДОВИ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕСЕНДЖЕРІВ ЗГІДНО СТАНДАРТУ OWASP MOBILE APPLICATION SECURITY

Проєкт OWASP Mobile Security – це техніка тестування безпеки мобільних програмних додатків. Він визначає ступінь серйозності найнебезпечніших вразливостей, а також стандартні та тестові сценарії та інструменти для оцінки безпеки. Структура проекту OWASP Mobile Security є взаємопов'язаною, наприклад, рейтинг OWASP Mobile TOP 10 найважливіших вразливостей базується на тестах, проведених відповідно до стандарту тестування. Однак на офіційній сторінці OWASP це не визначено належним чином. Точніше кажучи наведено лише схему взаємодії між стандартом, сценаріями тестування та інструментом для визначення оцінки вразливості ([39], рис 3.1):

- Контрольний список (Checklist) – це інструмент для обчислення рівня безпеки та захищеності, який потім відображається на графіках. Це дозволяє створювати зони з підвищеним рівнем безпеки.
- Вимоги (Requirements) – стандарт перевірки безпеки мобільних додатків (MASVS) використовується для підвищення та перевірки рівня безпеки мобільних програмних додатків.
- Тестові випадки (Test Cases) – посібник з тестування мобільної безпеки (MSTG) визначає стандартні тести для кожного етапу, які описані в MASVS і складаються з загальних Android та iOS частин.

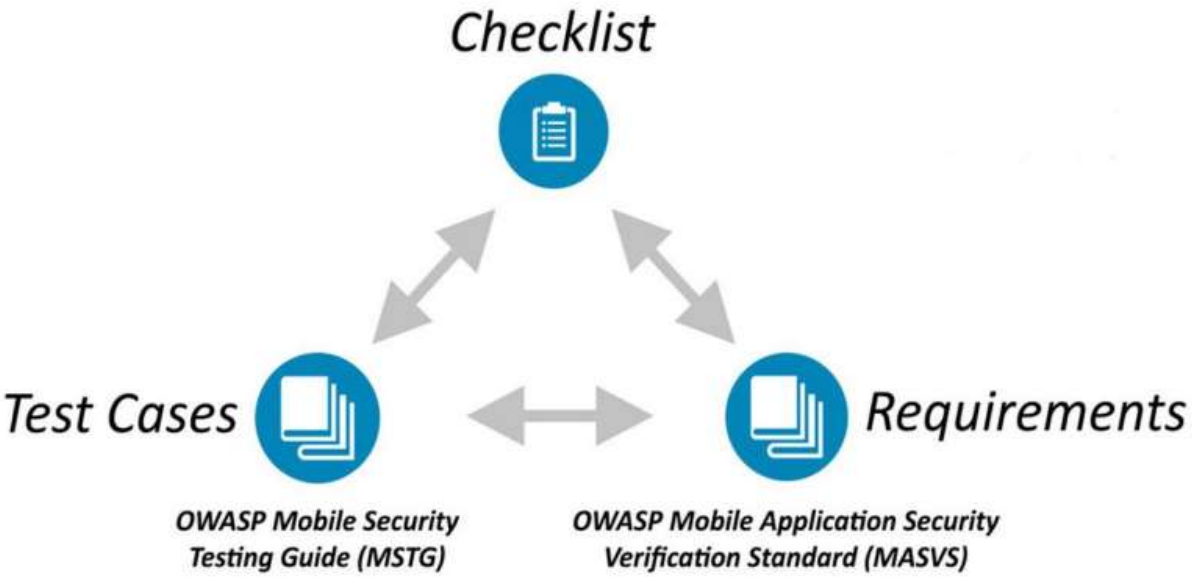

Рис. 3.1 Взаємодія між структурними елементами OWASP Mobile Security

Рівень безпеки мобільних додатків перевіряється відповідно до стандарту OWASP MASVS (OWASP Mobile Application Security Verification Standard). Він використовується як для визначення, так і для перевірки рівня безпеки. Стандарт був розроблений для досягнення цілей таких, як основа для тестування, переліку вимог для сертифікацій, метаданих.

3.1 Аналіз Мобільних ризиків за версією OWASP

На рис. 3.2 відображена порівняльна таблиця десяти головних мобільних ризиків за версією OWASP за 2024 рік ([40].

Comparison Between 2016-2024		
OWASP-2016	**OWASP-2024-Initial Release**	**Comparison Between 2016-2024**
M1: Improper Platform Usage	M1: Improper Credential Usage	New
M2: Insecure Data Storage	M2: Inadequate Supply Chain Security	New
M3: Insecure Communication	M3: Insecure Authentication / Authorization	Merged M4&M6 to M3
M4: Insecure Authentication	M4: Insufficient Input/Output Validation	New
M5: Insufficient Cryptography	M5: Insecure Communication	Moved from M3 to M5
M6: Insecure Authorization	M6: Inadequate Privacy Controls	New
M7: Client Code Quality	M7: Insufficient Binary Protections	Merged M8&M9 to M7
M8: Code Tampering	M8: Security Misconfiguration	Rewording [M10]
M9: Reverse Engineering	M9: Insecure Data Storage	Moved from M2 to M9
M10: Extraneous Functionality	M10: Insufficient Cryptography	Moved from M5 to M10

Рис. 3.2 Порівняльна таблиця між 2016-2024 роками

M1: Improper Credential Usage – неправильне використання облікових даних.

Ризик, який виникає, коли розробники мають неналежне управління обліковими даними (логіни, паролі, токени або ключі API). Часто такі облікові дані залишаються “зашитими” безпосередньо у коді програми, у конфігураційних файлах або зберігаються без шифрування в пам’яті пристрою. Це означає, що будь-який, хто отримає копію застосунку або доступ до файлової системи пристрою, може витягнути ці дані та скористатись ними для несанкціонованого доступу.

OWASP зазначає, що такі помилки часто виникають через зручність або поспіх під час розробки, коли програмісти тимчасово додають ключі в код і забувають їх прибрати. Правильний підхід полягає в тому, щоб використовувати безпечні сховища (Android Keystore чи IOS Keychain), уникати хардкодингу, застосовувати тимчасові токени з обмеженим строком дії та проводити регулярну ротацію ключів [40].

M2: Inadequate Supply chain Security – недостатня безпека ланцюга постачання.

Сучасні мобільні застосунки майже завжди базуються на сторонніх бібліотеках, SDK і фреймворках, які значно спрощують розробку, але разом з цими компонентами у систему може потрапити вразливий або навіть шкідливий код. Випадки, коли скомпрометовані пакети потрапляли до офіційних репозиторіїв, не поодинокі.

OWASP пояснює, що ця загроза не лише про вразливі залежності, а й про весь процес роботи – від підпису коду до публікації в магазині застосунків. Якщо хтось отримає контроль над інструментом збірки або ключем підпису, він може модифікувати додаток, не змінюючи його цифрового підпису. Для зменшення цього ризику необхідно контролювати походження всіх бібліотек, використовувати інструменти аналізу складу ПЗ (Software Composition Analysis),

регулярно оновлювати залежності та зберігати ключі підпису у захищених сховищах [40].

M3: Insecure Authentication / Authorization – небезпечна аутентифікація та авторизація.

Цей ризик стосується ситуацій, коли система перевірки особи або прав доступу реалізована некоректно. Наприклад, застосунок може довіряти клієнтській стороні для перевірки токенів чи ролей користувачів, тоді як ці перевірки завжди повинні виконуватись на сервері. Інші поширені помилки – це відсутність тайм-аутів сесій, слабкі паролі без політик складності або можливість "форс браузингу" – прямого доступу до прихованих API. У таких умовах зловмисник може увійти під чужим обліковим записом та отримати доступ до функцій адміністратора.

OWASP наголошує, що для уникнення цього потрібно використовувати стандартизовані механізми, наприклад, OAuth 2.0, JWT із перевіркою підпису, контроль життєвого циклу сесій і централізовану авторизацію на сервері [40].

M4: Insufficient Input/Output Validation – недостатня перевірка введення й виведення.

Вразливості цього типу виникають, коли мобільний застосунок приймає або обробляє дані без достатньої перевірки, наприклад, введення користувачем спеціальних символів або великої кількості даних може призвести до SQL-ін'єкції, переповнення буфера або виконнання небажаних команд. Те саме стосується й вихідних даних – якщо програма передає дані без фільтрації, вони можуть використовуватись для XSS або витоку конфіденційної інформації.

OWASP радить застосувати суворі правила валідації, наприклад, перевіряти довжину, тип, формат, а також очищати дані перед виведенням. Ключовим є принцим – недовіряй жодному введенню, навіть якщо воно походить із внутрішнього компонента застосунку [40].

M5: Insecure Communication – небезпечна комунікація.

Мобільні застосунки постійно обмінюються даними з віддаленими серверами, але часто цей обмін не належно захищений. Якщо передача відбувається через незашифрований канал або TLS налаштований неправильно, зловмисник може перехопити трафік і отримати доступ до паролів, токенів або особистої інформації.

OWASP звертає увагу на те, що навіть використання HTTPS не гарантує безпеку, якщо не перевіряється сертифікат сервера або дозволено старі версії TLS. Також важливо шифрувати не лише інтернет-трафік, а й передачу через Bluetooth, NFS чи інші протоколи. Рекомендація – використовувати сучасні шифри, застосовувати пінінг сертифікатів, забороняти незахищені з'єднання й ретельно перевіряти всю мережеву взаємодію [40].

M6: Inadequate Privacy Controls – недостатні засоби захисту приватності.

Цей ризик стосується того, як застосунок збирає, зберігає та обробляє персональні дані користувача. OWASP зазначає, що навіть якщо технічно все працює безпечно, порушення принципів приватності може створити серйозні проблеми. Часто додатки збирають більше даних, ніж потрібно, не повідомляють користувача про це або не надають можливості керувати своєю інформацією. Інколи персональні дані потрапляють у журнали, аналітику або кеш і залишаються там навіть після видалення. Правильний підхід полягає у мінімізації збору даних, шифруванні всіх персональних записів, впровадженні механізмів видалення, а також у дотриманні законодавства (GDPR, CCPA). Користувач повинен мати чітке розуміння, які саме дані обробляються і навіщо [40].

M7: Insufficient Binary Protections – недостатній захист бінарного коду.

Реверс-інжиніринг мобільних застосунків – це звичайна практика для зловмисників. Якщо код не обфускований, його можна легко декомпліювати, знайти логіку перевірок, ключі, паролі або навіть змінити поведінку програми.

Застосунок без внутрішніх перевірок цілісності можна змінити та знову підписати, створити підроблену версію, що виглядає справжньою.

OWASP пояснює, що для захисту потрібно впроваджувати обфускацію, мінімізувати відкрите відображення класів і методів, використовувати контроль цілісності, а також розділяти критично важливий код, наприклад, виконувати частину операцій на сервері. Мета – ускладнити аналіз і модифікацію настільки, щоб атака стала економічно невигідною [40].

M8: Security Misconfiguration – неправильна конфігурація безпеки.

Ця проблема охоплює безліч дрібних, але небезпечних помилок від активного debug-режиму у релізній версії до неправильного встановлених дозволів для файлів або компонентів Android. Наприклад, якщо Activity чи Service позначені як “exported”, будь-який інший додаток може запустити їх і взаємодіяти без авторизації. Також вразливими є відкриті API, неправильні політики CORS, незашифровані конфігураційні файли та тестові інтерфейси, залишені в продакшн.

OWASP підкреслює, що безпечна конфігурація – це не разова дія, а процес. Розробники мають створювати контрольні списки для збірки, вимикати перед релізом і періодично перевіряти конфігурацію через автоматизовані інструменти або пентести [40].

M9: Insecure Data Storage – небезпечне зберігання даних.

Багато мобільних додатків зберігають інформацію на пристрої користувача – це можуть бути токени доступу, паролі, історія дій ібо дані профілю. Якщо вони зберігаються у відкритому вигляді, їх можна витягнути навіть через резервні копії чи файлову систему. У випадку з Android дані іноді зберігаються у Sharedprefences без шифрування, у iOS у звичайних plist-файлах.

OWASP наголошує, що така практика є вкрай небезпечною, адже користувач може втратити телефон або його можуть взламати. Тому потрібно зберігати чутливу інформацію лише у захищених сховищах, шифрувати дані з

використанням сучасних алгоритмів і видаляти їх після завершення сесії або виходу користувача [40].

M10: Insufficient Cryptography – недостатня або неправильна криптографія.

Цей ризик пов’язаний із використанням слабких або неправильно реалізованих криптографічних алгоритмів. Деякі розробники створюють власні методи шифрування або використовують застарілі стандарти, які вже давно не забезпечують належного рівня безпеки. Інші помилки включають занадто короткі ключі, неправильне управління їхнім життєвим циклом або відсутність перевірки цілісності зашифрованих даних. У результаті дані можна розшифрувати або підробити.

OWASP радить застосовувати перевірені криптографічні бібліотеки, використовувати сучасні алгоритми (AES-GCM, ChaCha20, RSA, ECC), забезпечити належне управління ключами (створення, зберігання, ротацію) і ніколи не реалізовувати власну криптографію вручну [40].

Виходячи з зазначеного вище, OWASP підкреслює, що ці десять ризиків не існують ізольовано. Вони взаємопов’язані: неправильна аутентифікація часто йде разом із небезпечною комунікацією, а слабке шифрування - з поганим зберіганням даних. Безпечна мобільна розробка – це системний підхід, який починається з розумінням ризиків, дотримання найкращих практик безпеки та регулярного тестування додатків на наявність вразливостей [40].

В табл. 3.1 зазначено експлуатаційна спроможність зловмисників використати ту чи іншу вразливість, поширеність вразливості, технічні наслідки вразливості та спроможність виявлення розробниками зазначених вразливостей [40].

Таблиця 3.1

Ризики мобільних вразливостей

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
Вектор атаки (експлуатаційна спроможність)	Легка	Середня	Легка	Важка	Легка	Середня	Легка	Важка	Легка	Середня
Слабкість безпеки (поширеність)	Звичайна	Звичайна	Звичайна	Звичайна	Звичайна	Звичайна	Звичайна	Звичайна	Звичайна	Звичайна
Слабкість безпеки (виявлення)	Легке	Важке	Середнє	Легке	Середнє	Легке	Легке	Легке	Середнє	Середнє
Технічні наслідки (вплив)	Сильний	Сильний	Сильний	Сильний	Сильний	Низький	Помірний	Сильний	Сильний	Сильний

3.2 Проєктування системи шифрування повідомлень

Основне завдання ЗМВР спроєктувати стійку криптографічну систему для забезпечення конфіденційності усіх повідомлень користувачів. Стандарт OWASP MASVS у групі MASVS-CRYPTO визначає чіткі вимоги використання сучасних і стійких алгоритмів та коректного управління ключами протягом усього їхнього життєвого циклу. Так як мобільні пристрої значно вразливіші до фізичного доступу через втрату, викрадення або атаки через зловмисні застосунки, на відміну від серверів, це створює серйозну загрозу для даних, якщо вони не будуть належно зашифровані.

Месенджери зобов’язані впроваджувати наскрізне шифрування при якому ключі створюються та зберігаються виключно на пристроях користувачів і ніколи

не передаються на сервер у відкритому вигляді. Даний підхід навіть робить неможливим доступ адміністратору сервісу до вмісту повідомлень. На цей час сучасні месенджери вже реалізують протоколи схожі на Signal Protocol, які базуються на поєднанні асиметричної криптографії (для обміну ключами) та симетричної (для швидкого та безпечного шифрування).

MASVS-CRYPTO наголошує, що навіть сильна криптографія може бути повністю зруйнована при неправильному управлінні ключами. Через це проєктування системи повинно передбачати генерацію ключів у захищених контейнерах операційної системи таких, як iOS Secure Enclave або Android Keystore, це гарантує захист ключів від копіювання чи модифікації. Важливо реалізувати механізми ротації ключів, потрібна регулярна заміна при створенні нових сесій, знищення ключів після завершення використання або виходу з облікового запису.

Важливо враховувати особливості середовища з'єднання для шифрування повідомлень. Повідомлення передаються через мережу, де можливі атаки MITM. Через це MASVS рекомендує завжди використовувати TLS для передачі даних, а для критично вразливих систем додатково застосовувати сертифікаційний пінінг, який дозволяє впевнитися, що застосунок спілкується тільки з довіреним сервером задля виключення можливості підміни сертифіката зловмисником у разі компроментації кореневого центру сертифікації.

Отже стандарт MASVS зобов'язує притримуватись архітектури шифрування в месенджері та включати основні компоненти такі, як застосування сучасних алгоритмів, коректне управління ключами та мати захищені канали зв'язку. Ця комплексна система гарантує приватність повідомлень, що залишаться недоторканою навіть у випадку втрати пристрою, компроментації мережі чи злому серверної інфраструктури.

3.3 Розробка механізмів аутентифікації та авторизації

Фундаментальним елементом безпеки для месенджера є аутентифікація та авторизація. Стандарт OWASP MASVS у групі MASVS-AUTH визначає вимоги до цих процесів.

MASVS наголошує на застосуванні захищених протоколів аутентифікації та авторизації. Коли справа йде про аутентифікацію, то сучасні месенджери пропонують варіанти реалізації через пароль, одноразовий код або SMS-повідомлення чи e-mail, також можлива інтеграція з OAuth 2.0. Тим не менш будь яка реалізація повинна враховувати ризики перехоплення даних і тим самим забезпечувати їх передавання тільки через захищенні канали TLS. Стандарт MASVS чітко пояснює, що збереження паролів у відкритому вигляді або у форму, що допускає швидке відновлення, категорично недопустиме. Використання функції хешування з адаптивними алгоритмами bcrypt, scrypt, Argon2 є обов'язковими.

Наступним рівнем безпеки є локальна аутентифікація. Більшість сучасних месенджерів мають функцію блокування доступу до листувань шляхом біометрії або PIN-кодом і правильність реалізації цього механізму визначить, наскільки легко стороння особа зможе скористуватися вже авторизованим застосунком. MASVS-AUTH-2 наполягає, щоб такі механізми були узгоджені з найкращими практиками конкретної платформи, на iOS це Touch ID або Face ID з використанням Secure Enclave, на Android це стандартні API для біометрії, які гарантують, що дані відбитків обличчя чи пальців не будуть доступні розробнику.

MASVS-AUTH-3 вимагає додаткової аутентифікації для виконання критичних дії. Такими діями в месенджерах є зміна пароля, додавання нового пристрою, відновлення доступу, видалення акаунту або експорт ключів шифрування. Для цього стандарт рекомендує використовувати двофакторну авторизацію, це може бути як окремий додаток, який генерує коди, наприклад, Google Authenticator або через код підтвердження. Ці дії ускладнюють доступ до інформації зловмисником навіть, якщо він знає пароль користувача.

Усі дії, які вимагає стандарт, створять багаторівневу систему аутентифікації та авторизації, що в свою чергу створить зручність та захист для користувача та відповідність до вимог безпеки. Для будь-якого месенджера цей підхід є дуже важливим в плані надійності для користувачів та самого месенджера, адже, якщо зловмисник в разі злому отримає доступ до облікового запису та повідомлень, то зможе отримати доступ до інфраструктури обміну ключами, як висновок це повністю зруйнує конфіденційність системи месенджера.

3.4 Заходи з захисту від вірусів та шкідливих програм

OWASP MASVS зазначає, що захист на мобільних пристроях від шкідливого програмного забезпечення має принципово інший характер. Антивіруси, які існують для персональних комп’ютерів, не підходять для смартфонів через архітектури операційних систем Android та iOS. Це пояснює, чому неможливо реалізувати традиційний антивірус безпосередньо в месенджері.

MASVS-CODE має низку контролів, які спрямовані саме на запобігання використання вразливостей чи шкідливого коду. Перш за все застосунок має працювати на актуальних версіях операційних систем. Завдяки цьому користувач отримує останні патчі безпеки, що зменшує ризик використання вже відомих вразливостей. Додатково, сам месенджер повинен мати механізм оновлень задля того ж запобігання можливих вразливостей, які були виявлені. Для месенджера це є пріоритетним завданням через конфіденційність листувань користувачів, які відбуваються кожен день.

Ще один важливий фактор – це контроль використання сторонніх компонентів, бібліотек та SDK. Сучасні мобільні застосунки значною мірою базуються на сторонньому коді і це створює ризик поширення вразливостей через ланцюжок постачання. Вимоги MASVS перевіряти всі бібліотеки на наявність вразливостей через автоматизовані системи типу SCA та відмовлятися в використані у випадку виявлення проблем. У випадку з месенджерами варто бути пильним та приділяти достатню увагу криптографічним бібліотекам та механізмам обробки мультимедіа бо саме вони найчастіше стають цілями для атак.

Окрім вище зазначеного ще необхідна валідація та санітизація даних, що надходять в месенджер. Будь які повідомлення, файли, посилання чи аватари можуть містити недоречний або шкідливий зміст. Якщо месенджер не перевіряє ці данні, то зловмисники можуть спокійно проводити фішинг або інші атаки, тим самим викрадати дані користувачів. Правильна обробка даних дозволяє захистити месенджер від використання його для поширення шкідливого програмного забезпечення.

Отже вимоги MASVS до стратегії регулярних оновлень, контролю та відмов від небезпечних бібліотек та правильної обробки даних, які надходять від користувачів, дозволяють створити систему, яка буде стійка до інфекцій у середовищі з активним користуванням та можливим розповсюдженням шкідливого програмного забезпечення.

3.5 Створення системи аналізу та блокування загроз у режимі реального часу

Завершаючий етап безпеки месенджера, який розглядає стандарт OWASP MASVS, стосується стійкості до загроз та реагування на них у реальному часі. MASVS-RESILIENCE визначає низку вимог, спрямованих на протидію реверс-інжинірингу, тамперингу та динамічному аналізу та на перевірку цілісності середовища месенджера.

Месенджер є одним з найпріоритетніших цілей для зловмисника через обсяг приватних повідомлень користувачів. Відповідно вимогам MASVS-RESILIENCE-1 в пристроях, в яких вносили зміни для збільшення прав, обходу офіційних сервісів для скачування програм та інших змін, які зроблені вручну для збільшення привілеїв, знижується рівень гарантій безпеки. Тому застосунок має мати можливість виявляти скомпрометовані пристрої та повідомляти користувача чи за необхідності блокувати роботу месенджера.

Також зловмисник може спробувати створити підроблену версію месенджера, ця версія може містити в собі функції стеження за голосом, відео, файлами та

іншими діями користувача, що є порушенням конфіденційності. Тому захист від модифікації застосунку є важливим елементом безпеки. Механізми анти-тамперингу MASVS-RESILIENCE-2 дозволяють перевіряти цілісність коду та ресурсу під час запуску та у процесі роботи, тим самим блокуючи можливі, сторонні зміни.

MASVS-RESILIENCE-3 та MASVS-RESILIENCE-4 наголошують на необхідності протидії статичному та динамічному аналізу. Це означає, що розробник ЗМВР повинен ускладнювати процес зворотного аналізу, прикладом є обфускація коду, шифрування рядків, вбудовані перевірки на несправності. Завдяки цим протидіям зловмиснику складніше зламати або модифікувати застосунок.

Таким чином, вимоги MASVS-RESILIENCE поєднують в собі перевірки цілісності середовища, захист від реверс-інжинірингу та механізми реагування на підозрілу активність. Дотримуючись стандарту MASVS, ЗМВР стане надійним і дозволить користувачам довіряти сервісу в умовах складного кіберсередовища.

Загалом стандарт OWASP MASVS має всі вимоги для створення розробником безпечного середовища для користувачів ЗМВР. Дотримання вимог шифрування допоможе в конфіденційності та надійності користування, аутентифікація та авторизація зробить застосунок більш безпечним для користування і у разі втрати носія даних користувач може не перейматися за викрадення/прочитання персональних даних та особистих листувань, заходи від вірусів та шкідливих програм за стандартом ясно дають зрозуміти, що додаток треба постійно оновлювати, код месенджера має бути якісним та не мати щілин для втручання в нього, система захисту у режимі реального часу, яка описана у OWASP MASVS, підкреслює, що ЗМВР повинен вміти виявляти небезпечне середовище, захищати себе від змін і підробки та ускладнювати спроби зламу або модифікації.

Висновки до третього розділу

З урахування проведеного аналізу мобільних ризиків за версією OWASP розробнику рекомендується при проєктуванні систем безпеки ЗМВР орієнтуватися на принцип побудови багаторівневого захисту, що охоплює всі етапи життєвого циклу програмного продукту – від архітектури до експлуатації. Особливу увагу слід приділити усуненню найкритичніших загроз, визначених OWASP, серед яких: витік даних, вразливості автентифікації, ненадійне зберігання конфіденційної інформації та ризики, пов’язані з неконтрольованим доступом до API.

Розробник повинен впроваджувати сучасні алгоритми шифрування для забезпечення конфіденційності обміну повідомленнями, використовувати багатофакторну автентифікацію та гнучкі механізми авторизації, що унеможливлюють несанкціонований доступ до даних користувачів. Доцільним є створення інтегрованої системи моніторингу стану безпеки, здатної аналізувати мережеву активність у реальному часі, виявляти підозрілі дії та блокувати потенційні загрози це до їх реалізації.

Рекомендовано дотримуватись принципів «security by design» та «privacy by default», які передбачають закладення механізмів захисту ще на етапі проєктування системи. Для підвищення рівня надійності криптографічних рішень та перевірки відповідності вимогам українського законодавства у сфері технічного та криптографічного захисту інформації доцільно залучати спеціалізовані українські компанії – ТОВ «АВТОР», ТОВ «ТРИТЕЛ» та ТОВ НВФ «Криптон», які мають досвід у побудові комплексних систем кібербезпеки та сертифікованих засобів захисту інформації.

ВИСНОВКИ

У роботі було розглянуто процеси забезпечення безпеки застосування месенджерів на мобільних пристроях. Базуючись на проведеному досліджені було визначено, що на сьогодні є загальнодержавна потреба у безпечному месенджері української розробки.

Розробка захищеного месенджера вітчизняної розробки (ЗМВР) потребує комплексного підходу у якому захист інформації розглядається не як окремий елемент, а як невід'ємна частина всієї архітектури. У сучасних умовах мобільні застосунки стають основною мішенню для кіберзлочинців, а тому створення надійного засобу комунікації потребує продуманого впровадження всіх механізмів безпеки – від криптографії до контролю зберігання даних, управління ризиками та постійного моніторингу якості коду. Водночас українське законодавство вимагає, щоб розробник, який створює продукт із вбудованими криптографічними засобами, мав чинну ліцензію на діяльність у сфері криптографічного захисту інформації. Наявність такої ліцензії гарантує, що розробник володіє необхідними компетенціями, дотримується принципів регульованого захисту, використовує дозволені механізми шифрування та впроваджує систему внутрішнього контролю. У разі орієнтації ЗМВР на державний сектор ліцензійність та відповідність національним вимогам стають вимогою безальтернативною.

Безпека ЗМВР повинна ґрунтуватись на захисті конфіденційності, цілісності та доступності даних [46, 47]. Конфіденційність забезпечується наскрізним шифруванням, яке унеможливлює доступ до вмісту повідомлень стороннім особам. Цілісність передбачає захист від змін даних під час їх передавання або зберігання. Доступність гарантує безперебійну роботу сервісу, щоб користувач завжди мав змогу отримати свої повідомлення та встановити зв'язок. Такі принципи лежать в основі всіх сучасних комунікаційних систем і визначають необхідність продуманого підходу до побудови архітектури.

Окрім захищеного протоколу шифрування, важливо, щоб ЗМВР не зберігав чутливі дані у незахищеному вигляді. Мобільні пристрої мають власні механізми

захищених сховищ і ЗМВР повинен використовувати їх для конфіденційної інформації: ключів шифрування, токенів доступу, локальних баз даних. Необхідно забезпечити, щоб застосунок не залишав конфіденційні дані у фоні та не відображав їх у системних знімках екрану, які можуть бути доступні іншим програмам. Важливо, щоб ЗМВР блокував запуск на рутованих чи скомпрометованих пристроях, оскільки такі пристрої не можуть гарантувати захист файлової системи та пам’яті.

Мережевий захист є ще одним критично важливим компонентом. Трафік між клієнтом та сервером має передаватися винятково в зашифрованому вигляді з використанням сучасних версій захищених протоколів і додаткових механізмів перевірки, такими як перевірка справжності серверного сертифіката. У випадку обходу таких перевірок зловмисник може перехопити трафік. Отримати доступ до службових даних або змінити вміст переданої інформації. Тому важливим завданням розробника є впровадження надійного контролю мережевих з’єднань та стійкість до атак типу MITM.

Дуже поширеним джерелом загроз є стороні бібліотеки. Мобільні застосунки часто використовують готові компоненти, але за умови їх неналежної перевірки існує ризик, що бібліотека може містити уразливість або прихований шкідливий код. Тому розробник повинен проводити контроль залежностей, аналізувати їх актуальність, перевіряти рівень безпеки кожного компонента перед релізом і регулярно оновлювати їх після інтеграції в продукт.

Для забезпечення високої стійкості системи необхідно впроваджувати перевірку цілісності застосунку, щоб унеможливити його модифікацію. Обфускація коду, перевірка підпису, виявлення дебаг-інструментів та сторонніх програм аналізу створить додаткові перешкоди для зловмисника, який захоче дослідити внутрішню логіку застосунку або змінити його поведінку.

Важливою частиною забезпечення безпеки є проведення регулярних перевірок. Вони повинні охоплювати як статичний аналіз коду, що дозволяє виявити помилки на ранніх етапах, так і динамічне тестування, що дозволяє

виявити логічні та поведінкові вразливості вже під час роботи ЗМВР. Ефективність таких перевірок значною мірою залежить від того, наскільки розробник системно підходить до управління ризиками, відстеження змін, перевірки нових функцій та тестування оновлень. Оскільки мобільні застосунки постійно змінюються, а платформи отримують нові версії, оцінка безпеки має проводитися не разово, а циклічно, із включенням у процес життєвого циклу розробки. Таким чином забезпечується ефективна адаптація механізмів захисту до нових умов.

Також важливо враховувати організаційні вимоги українського законодавства, пов’язані зі збереженням персональних даних, повідомленням про інциденти, захистом службової інформації та дотриманням вимог використання засобів захисту. Усі ці аспекти формують додаткові критерії за якими повинен оцінюватися майбутній ЗМВР. Продукт, який претендує на використання у державному або корпоративному секторі має відповідати цим критеріям і мати достатні засоби контролю доступу, журналювання, відновлення після збоїв та протидії внутрішнім загрозам.

У результаті – створення українського ЗМВР це не просто розробка алгоритму шифрування, а побудова цілісної системи, що включає захист програмного забезпечення, інфраструктури, каналів зв’язку, логіки автентифікації, сховищ даних, а також відповідність нормативним вимогам. Лише поєднання ліцензованої діяльності, сучасних практик безпеки, ретельного контролю коду, регулярного тестування, аналізу ризиків та безперервного вдосконалення дозволяє створити продукт, який забезпечує високий рівень довіри та ретельний захист приватної комунікації у сучасному середовищі кіберзагроз.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [48].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тарасюк А.В. Система суб'єктів забезпечення кібербезпеки в Україні. *Адміністративне право і процес; фінансове право інформаційне право.Т.31(70) Ч.2. № 2. 2020. С. 119-124.* URL: https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_2/25.pdf .

2. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

3. Правова база української кібербезпеки: загальний огляд і аналіз. URL:https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf.

4. Проект Закону про внесення змін до Закону України «Про Службу безпеки України» щодо удосконалення організаційно-правових засад діяльності Служби безпеки України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68347

5. Snort. URL: https://www.snort.org/.

6. Досвідчені фахівці, сучасні технології та співпраця – ключові компоненти для побудови надійного кіберзахисту. *Державна служба спеціального зв'язку та захисту інформації України. Новини 17.02.2025 р.* URL: https://cip.gov.ua/ua/news/experienced-professionals-modern-technologies-and-collaboration-key-components-for-building-robust-cyber-defense.

7. WEZOM. 6 трендів кібербезпеки в 2024 році. URL: https://wezom.com.ua/ua/blog/6-trendiv-kiberbezpeki-v-2024-rotsi.

8. Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics. URL: https://cybersecurityventures.com/cybersecurity-almanac-2023/.

9. Artificial Intelligence and Cybersecurity Research. URL: https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research.

10. Як працює блокчейн та де використовують цю технологію, окрім криптовалюти та NFT. URL: https://robotdreams.cc/uk/blog/635-how-blockchain-works?utm_term=&utm_campaign=blog&utm_source=google&utm_medium=cpc&utm_content=pmax_ua&hsa_acc=9854447533&hsa_cam=22491897308&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tgt=&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_source=1&gad_campaignid=22495379017&gbraid=0AAAAACP7rf6pAJGkx9wiJxH2p1BmZNNyO&gclid=Cj0KCQjwyvfDBhDYARIsAItzbZFBHBYuZVA54vYqzRKvPlptz2xAeS7pnkciqJ5OmAZpPBjoMET3Pg4aApXSEALw_wcB.

11. Що таке IPS/IDS і де застосовується. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya.

12. Що таке кінцева точка? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-an-endpoint.

13. Що таке MFA — багатофакторна аутентифікація? URL: https://datami.ee/ua/blog/shho-take-mfa-bagatofaktorna-autentifikatsiya/.

14. Що таке багатофакторна автентифікація (MFA)? URL:https://cloud.smart-it.com/news-post/what-is-mfa/.

15. Системи Моніторингу Безпеки. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/security-monitoring-systems?srsltid=AfmBOorQbNcvzquxitUBuadyX3qnaTZLGz6Ac2RA9Lde6KnS9HcXf_Q2.

16. Крет Ольга, Крет Роман, Кундеус Оксана. Система кібербезпеки як складова національної безпеки держави. *ГРАНІ. Т. 27. №5. 2024. С.92-99.* DOI: https://doi.org/10.15421/172496. URL: https://grani.org.ua/index.php/journal/article/view/2092/2060.

17. Сліпченко, Т. (2020). Кібербезпека як складова системи захисту національної безпеки: європейський досвід. *Актуальні проблеми правознавства.* 1 (21)/2020. С.128 – 133. ISSN 2524-0129 (Print) / ISSN (2664-5718) (Online). DOI:10.35774/app2020.01.128. URL: https://dspace.wunu.edu.ua/bitstream/316497/38497/1/%D0%A1%D0%BB%D1%96%D0%BF%D1%87%D0%B5%D0%BD%D0%BA%D0%BE.pdf.

18. Ліпкан, В., Діордіца, І. (2017). Національна система кібербезпеки як складова частина системи забезпечення національної безпеки україни. *Підприємництво, господарство і право, № 5. 2017. С. 175-180.* 4. URL: http://pgp-journal.kiev.ua/archive/2017/5/40.pdf.

19. Мужанова Т., Легомінова С., Щавінський Ю., Якименко Ю., Нестеренк Г. (2024). ОСНОВНІ ПІДХОДИ Й НАПРЯМИ РОЗВИТКУ ПОЛІТИКИ КІБЕРБЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 4(24), 133–149. URL: https://doi.org/10.28925/2663-4023.2024.24.133149.

20. Стівенс, Д. Т., Бертон, Д. Дж. (2023). НАТО і стратегічна конкуренція в кіберпросторі. *НАТО Ревю.* 06 червня 2023. URL: https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna-konkurentsya-v-kberprostor/index.html.

21. Найпопулярніші види кібератак у 2021. URL: https://10guards.com/ua/blog/2021/07/08/the-most-common-types-of-cyber-attacks-in-2021/.

22. Бурячок В.Л., Гнатюк С.О., Корченко О.Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. Інформаційна безпека: виклики і загрози сучасності: *зб. матеріалів наук.-практ. конф., 5 квітня 2013 р., м. Київ*. Київ: Наук.-вид. центр НА СБ України, 2013. 416 с.

23. Рейтинг месенджерів 2025 року: оцінюємо безпеку, конфіденційність та функціонал. NGO "OSINT", 2025. URL: https://www.molfar.institute/rejtyng-mesendzheriv-2025-roku-oczinyuyemo-bezpeku-konfidenczijnist-funkczional/

24. WhatsApp. URL: https://uk.wikipedia.org/wiki/WhatsApp .

25. Facebook Messenger.
URL: https://uk.wikipedia.org/wiki/Facebook_Messenger

26. Snapchat.
URL:https://uk.wikipedia.org/wiki/Snapchat#:%20~:text=Snapchat%%2020(%D0%A1%D0%BD%D0%B5%D0%BF%D1%87%D0%B0%D1%82)%20%E2%80%94%20%D0%BC%D1%83%D0%BB%D1%8C%D1%82%D0%B8%D0%B

C%D0%B5%D0%B4%D1%96%D0%B9%D0%BD%D0%B8%D0%B9%20%D0%BC%D0%BE%D0%B1%D1%96%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9,%C2%ABSnapchat%20Inc.%C2%BB.

27. WeChat. URL: https://uk.wikipedia.org/wiki/WeChat.

28. QQ. URL: https://uk.wikipedia.org/wiki/QQ.

29. Wire. URL: https://bizmag.com.ua/mesendzhery/ .

30. Топ-10 месенджерів: аналоги Telegram. URL: https://vctr.media/ua/top-10-mesendzheriv-analogi-telegram-261935/.

31. Telegram. URL: https://uk.wikipedia.org/wiki/Telegram.

32. Приватність у мережі: який мессенджер захистить ваші дані? URL: https://cases.media/article/privatnist-u-merezhi-yakii-mesendzher-zakhistit-vashi-dani.

33. Опитування по месенджерами в Україні. URL: https://1news.com.ua/tsikave/nazvano-najpopulyarnishi-mesendzhery-v-ukrayini-2.html.

34. Viber. URL: https://uk.wikipedia.org/wiki/Viber.

35. Мінуси Telegram. URL: https://golos.kyivcity.gov.ua/bezpeka/zahrozy-ta-ryzyky-poviazani-z-vykorystanniam-mesendzhera-telegram?utm_source=chatgpt.com.

36. Новий супер-захищений мессенджер SimpleX Chat: переваги й недоліки. URL: https://censor.net/ua/blogs/3525466/novyyi-super-zahyschenyyi-mesendjer-simplex-chat-perevagy-yi-nedoliky.

37. WeChat: Китай без Google та Facebook та чому це важливо для українців. URL: https://www.vectorchina.biz/ua/blog/wechat-yak-v-kitai-obhodyatsya-bez-google-ta-facebook-ta-chomu-ce-vazhlivo-dlya-ukrainciv/.

38. Чи безпечний WeChat. URL: https://www.vpnunlimited.com/ ua/help/solutions/is-wechat-safe?srsltid=AfmBOopcBgEnDpzS6eS6ahYGBF-E1kB2RSDFin1Sa_i8sXzgrLcQvWct.

39. Антонішин, М. (2020). Модель тестування вразливостей мобільних застосунків. *Збірник «Інформаційні технології та безпека»,* 8(1), 49–57. URL: https://doi.org/10.20535/2411-1031.2020.8.1.218003

40. 10 головних мобільних ризиків - OWASP Mobile Top 10 2024 - Фінальний реліз. URL: https://owasp.org/www-project-mobile-top-10/2023-risks/

41. Дем'янчук А. ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ТРАФІКУ МЕСЕНДЖЕРІВ НА МОБІЛЬНИХ ПРИСТРОЯХ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ З БЕЗПЕКИ: зб. тез XII Всеукраїнської науково-практичної конференції молодих учених «Інформаційні технології – 2025», 15 травня 2025 р., м. Київ / КСУБГ. Київ: Київський столичний університет імені Бориса Грінченка, 2025, 278–279. ISSN: 2664-2638.

42. Дем'янчук А. Аналіз вразливостей та загроз безпеці інформації, що циркулює у мережах сучасних комунікаційних месенджерів: зб. тез доповідей конференції «Безпека інформаційно-комунікаційних систем. БІКС'2025», 26 жовтня 2025 р., м. Київ / КСУБГ. Київ: Київський столичний університет імені Бориса Грінченка, 2025, 45-49. URL: https://fitm.kubg.edu.ua/informatsiya/naukova-diialnist/konferentsii-fakultetu/2646-bezpeka-informatsiino-komunikatsiinykh-system.html

43. Наказ Державної служби спеціального зв'язку і захисту інформації України «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації» від 20.07.2007 № 141. URL: https://zakon.rada.gov.ua/laws/show/z0862-07#Text.

44. ТОВ «Трител». URL: http://www.tritel.ua/index.php/uk/pro-companiyu.

45.ТОВ «АВТОР». URL: https://avtor.ua/uk/about.

46. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Кібербезпека: освіта, наука, техніка, 1(25), 229–252. https://doi.org/10.28925/2663-4023.2024.25.229252

47. Крючкова, Л., & Стеблина, О. (2024). Захист смартфонів від впливу шкідливих програм в процесі зарядки у громадських місцях. Кібербезпека: освіта, наука, техніка, 3(23), 338–347. https://doi.org/10.28925/2663-4023.2024.23.338347

48. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для

студентів спеціальності 125 Кібербезпека та захист інформації. https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shevchenko_MR_Master_2023_FITM.pdf