УДК 614.84:004.056.5

С. В. Гончар, С. В. Стась, А. О. Майборода, О. В. Власенко

Національний університет цивільного захисту України

ЦИФРОВА БЕЗПЕКА У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ: ФУНКЦІОНУВАННЯ ЗАХИЩЕНИХ МЕСЕНДЖЕРІВ, АКТУАЛЬНІ ЗАГРОЗИ Й МЕТОДИ ЗАХИСТУ

У статті розглянуто питання цифрової безпеки у сфері цивільного захисту з акцентом на використанні захищених месенджерів під час оперативної діяльності рятувальників. Проаналізовано сучасні платформи обміну повідомленнями (Telegram, WhatsApp, Signal, Viber), їхню архітектуру, механізми шифрування та автентифікації, а також типові вразливості та методи атак, включно з фішингом, SIM-підмінами та атаками «нульового кліку». Проаналізоване експериментальне моделювання показало, що наскрізне шифрування і двофакторна автентифікація суттєво підвищують стійкість облікових записів до несанкціонованого доступу. Особливу увагу приділено практичному застосуванню захищених месенджерів під час виїзду пожежного автомобіля з оперативним розрахунком, де передача службової інформації про місце події, час прибуття, чисельність особового складу та залучену техніку має критичне значення для безпеки та ефективності операцій. Запропоновано комплекс заходів із використання E2EE, оновлених клієнтів, обмеження передачі чутливих даних та дотримання нормативних документів ДСНС для мінімізації кіберризиків та підвищення загальної кіберстійкості системи цивільного захисту.

Ключові слова: *цифрова безпека, цивільний захист, месенджери, захищені канали, E2EE, двофакторна автентифікація, оперативна інформація.*

The article addresses digital security in the field of civil protection, focusing on the use of secure messaging applications during emergency response operations by rescuers. Modern messaging platforms (Telegram, WhatsApp, Signal, Viber) are analyzed in terms of their architecture, encryption and authentication mechanisms, as well as typical vulnerabilities and attack methods, including phishing, SIM swap attacks, zero-click exploits, and metadata manipulation. Experimental modeling in a controlled environment demonstrated that the implementation of end-to-end encryption (E2EE) and two-factor authentication (2FA) significantly enhances account resilience against unauthorized access, even in cases of compromised communication channels or

mobile devices. Special attention is given to the practical use of secure messaging during the deployment of fire trucks with operational crews, where the transmission of operational information regarding incident location, arrival time, personnel count, and deployed equipment is critical for both safety and operational efficiency. The study emphasizes the necessity to limit the use of publicly accessible communication channels and comply with the regulatory framework of the State Emergency Service of Ukraine regarding the handling and transmission of operational information. Specific risk scenarios are considered, including potential interception of coordinates, route details, emergency response information, and other sensitive data that could be exploited by malicious actors to obstruct or mislead rescue operations. A set of measures to enhance cyber resilience is proposed: use of platforms with verified cryptographic architecture, activation of two-factor authentication for rescuers' accounts, limitation of device synchronization, deployment of updated client applications, and adherence to organizational regulations for handling sensitive data. Implementation of these measures minimizes the risk of interception or modification of operational information and ensures the protection of personal data while improving coordination efficiency in critical situations. The results highlight that digital security in civil protection is an integral component of operational resilience and rescuer safety. The recommended approaches can be applied to establish internal policies for secure use of digital communication channels within State Emergency Service of Ukraine, as well as to raise personnel awareness of modern cyber threats and protection methods. The study demonstrates that integrating technical and organizational security measures is essential for mitigating cyber risks and ensuring reliable transmission of operational information during emergency response activities.

Keywords: *digital security, civil protection, messaging applications, secure channels, E2EE, two-factor authentication, operational information.*

Вступ та постановка задачі. У сучасному цифровому середовищі месенджери стали ключовим інструментом щоденної комунікації – як у приватному житті, так і в професійній діяльності, зокрема у сферах безпеки та управління надзвичайними ситуаціями. Широке розповсюдження мобільних платформ спростило обмін інформацією, однак одночасно збільшило й кількість векторів для зловмисних дій. На цьому тлі стрімко зростає кількість кібератак, спрямованих на перехоплення персональних даних, компрометацію службових облікових записів, втручання в канали комунікації та поширення шкідливого програмного забезпечення через популярні сервіси миттєвих повідомлень.

Працівникам рятувальних підрозділів слід обмежувати використання месенджерів, а проведене дослідження стосується лише випадків крайньої необхідності, коли застосування таких засобів

комунікації є обґрунтованим та узгодженим із нормативними документами ДСНС. Особливої ваги питання безпечного використання месенджерів набуває у випадках їх застосування для координації дій під час ліквідації наслідків надзвичайних ситуацій, де значна частина інформації може бути чутливою або службовою. У системі ДСНС України швидкість передачі даних критично важлива, проте використання неперевірених або загальнодоступних каналів зв'язку створює додаткові ризики. Виявлені вразливості у таких застосунках, як WhatsApp, Telegram та інших популярних платформах, а також удосконалення технік фішингу, атак «нульового кліку», SIM-підміни та соціальної інженерії підсилюють необхідність поглибленого аналізу архітектури цих сервісів і їхніх слабких місць.

У зв'язку з цим працівникам ДСНС особливо важливо обмежувати використання месенджерів під час виконання службових обов'язків, адже безконтрольне чи нецільове застосування таких засобів може призвести до витоку оперативної інформації, розкриття персональних даних співробітників або ускладнення проведення рятувальних операцій. Якщо ж виникає потреба у використанні цифрових каналів комунікації, це повинно здійснюватися виключно з урахуванням чинних нормативних документів ДСНС, які регламентують порядок роботи з інформацією, обмеження щодо поширення даних, а також вимоги до технічних і організаційних заходів безпеки. Дотримання цих правил є необхідною умовою збереження конфіденційності, цілісності та доступності службових відомостей.

Таким чином, актуальність дослідження зумовлена потребою підвищення кіберстійкості як окремих користувачів, так і державних структур, що покладаються на цифрові канали зв'язку під час реагування на надзвичайні ситуації. Розуміння принципів функціонування месенджерів, оцінка типових ризиків, а також формування чітких рекомендацій щодо їх безпечного використання є важливим елементом зміцнення загального рівня інформаційної безпеки у сфері цивільного захисту.

Показовим прикладом сфери, у якій особливо важливо коректно та обмежено використовувати месенджери, є оперативна діяльність рятувальників під час виїздів на пожежі та інші надзвичайні події (виїзд пожежного автомобіля з оперативним розрахунком). Під час таких операцій передаються дані про місце події, час прибуття підрозділів, кількість залученого персоналу та техніки – інформація, що може бути використана зловмисниками для перешкоджання роботі рятувальників або для координації власних протиправних дій. Будь-яке стороннє

перехоплення таких відомостей створює ризики як для безпеки працівників, так і для ефективності ліквідації надзвичайної ситуації. Тому працівникам ДСНС критично важливо дотримуватися встановлених нормативних вимог щодо передачі оперативної інформації та уникати використання несанкціонованих цифрових каналів зв'язку під час виконання службових завдань.

Метою дослідження є аналіз принципів роботи сучасних месенджерів, їхньої архітектури, механізмів передачі даних та вбудованих систем захисту, а також виявлення типових вразливостей і методів атак, що можуть бути використані проти користувачів, зокрема працівників служб цивільного захисту. Особливий акцент робиться на оцінці рівня безпеки цих платформ у контексті їх потенційного застосування у критично важливих процесах ДСНС України, на ризиках, пов'язаних із неконтрольованим або ненормованим використанням цифрових засобів зв'язку, та на аналізі вимог чинних нормативних документів, які регламентують роботу з інформацією. Дослідження спрямоване на розробку практичних рекомендацій щодо підвищення безпеки службового обміну даними, мінімізації кіберзагроз і зміцнення загальної кіберстійкості системи цивільного захисту.

Основна частина. Метод. У межах дослідження було застосовано експериментальний метод, що передбачав моделювання типових кіберзагроз для сучасних месенджерів у контрольованому лабораторному середовищі. Для цього було створено тестову мережеву інфраструктуру, до якої підключалися пристрої з установленими популярними застосунками обміну повідомленнями (Telegram, WhatsApp, Signal, Viber). Дослідження передбачало оцінку можливостей перехоплення та модифікації даних у ненадійних мережах, аналіз стійкості до атак типу «людина посередині» та різновидів безклікових атак, а також перевірку механізмів захисту під час авторизації користувачів і встановлення сесій.

Результати дослідження. У ході експериментального дослідження встановлено, що рівень захищеності різних месенджерів суттєво варіює залежно від особливостей їх архітектури, використаних криптографічних механізмів та впроваджених методів автентифікації. Зафіксовано, що Signal продемонстрував найвищу стійкість до поширених моделей атак, включно зі спробами аналізу трафіку, фішинговими впливами та тестуванням у незахищених мережевих середовищах. Усі проведені випробування, засновані на імітації атак типу «людина посередині» (MITM), не призвели до розшифрування

вмісту повідомлень навіть за умов повного контролю над середовищем передачі даних.

Telegram виявив підвищену вразливість у межах використання звичайних чатів, де шифрування здійснюється за моделлю «клієнт–сервер». У контрольованому середовищі підтверджено можливість перехоплення окремих метаданих (зокрема інформації про підключення та характеристики пристрою), при цьому зміст повідомлень залишався недоступним для стороннього аналізу. WhatsApp продемонстрував високі показники захищеності текстових повідомлень, проте виявився схильним до ризиків, пов’язаних із коректністю обробки вкладених файлів у десктопному застосунку, що узгоджується з низкою описаних уразливостей, включно з CVE-2025-30401.

Viber дозволив перехоплювати частину метаданих, а під час передавання PDF-файлів спеціальних форматів продемонстрував несистемну активацію захисних механізмів, що може свідчити про окремі потенційні уразливості.

Проведене дослідження також підтвердило значущість двофакторної автентифікації (2FA) як критичного елементу захисту облікових записів. У всіх випадках, коли було активовано 2FA, моделювання атак, пов’язаних з перехопленням одноразових кодів підтвердження або порушенням цілісності SIM-карт, не дало змоги реалізувати несанкціонований доступ.

Узагальнені результати вказують на потребу підвищення рівня користувацької обізнаності щодо налаштувань безпеки та вдосконалення механізмів захисту на рівні настільних клієнтів і серверної обробки вкладень

Сучасні цифрові комунікації значною мірою ґрунтуються на функціонуванні месенджерів – програмних засобів, що забезпечують оперативний обмін повідомленнями між користувачами. Платформи, такі як Telegram, WhatsApp, Signal і Viber, застосовуються як у повсякденній взаємодії, так і у професійній діяльності, а також у межах окремих елементів оперативної координації, зокрема в системі ДСНС України. Їх поширення зумовлене поєднанням функціональної зручності та високої швидкості передавання даних. За простим інтерфейсом таких застосунків стоїть комплексна архітектура, що включає механізми маршрутизації, шифрування, автентифікації та забезпечення цілісності інформації. Відповідно важливим є аналіз внутрішньої організації таких систем, характерних моделей захисту та ролі допоміжних механізмів, зокрема двофакторної автентифікації, у забезпеченні стійкості до сучасних кіберзагроз.

Ключовою основою більшості месенджерів є клієнт-серверна архітектура, що складається з клієнтського застосунку, серверної інфраструктури та набору мережевих протоколів [1]. Клієнт забезпечує взаємодію з користувачем та первинну обробку інформації, сервери здійснюють маршрутизацію й тимчасове зберігання даних, тоді як протоколи зв'язку (HTTP/HTTPS, WebSocket або власні розробки, зокрема MTProto у Telegram) забезпечують передачу даних через мережу Інтернет.

Рис. 1 – Найпростіша типова схема надсилання повідомлення

Типова логіка роботи передбачає: надсилання повідомлення користувачем (рисунки 1, 2), його передавання на сервер за захищеним каналом, автентифікацію джерела, визначення одержувача та доставку на цільовий пристрій. За відсутності активного підключення одержувача сервер здійснює тимчасове зберігання даних у встановлений протоколами термін [2]. У децентралізованих архітектурах (наприклад, Matrix) функції розподіляються між кількома серверами, що підвищує загальну відмовостійкість.

Рис. 2 – Схема надсилання повідомлення із резервуванням

Важливою складовою є синхронізація між пристроями. Наприклад, WhatsApp застосовує механізм сканування QR-коду для поєднання мобільного та настільного клієнтів, тоді як Telegram використовує хмарну інфраструктуру, що забезпечує повну історію взаємодій незалежно від пристрою доступу [3]. Подібні рішення потребують оптимізованих механізмів серверного зберігання та обробки даних

Передавання повідомлень реалізується за допомогою комбінації мережевих протоколів. TCP/IP забезпечує гарантовану доставку, а WebSocket – двосторонню взаємодію в режимі реального часу. Протокол Signal Protocol, що застосовується в однойменному месенджері, використовує криптографічну модель подвійного ратчет-алгоритму (Double Ratchet) для забезпечення секретності сеансів [4]. Telegram поєднує HTTPS із власним протоколом MTProto. Передавання повідомлень здійснюється у формі структурованих даних (наприклад, JSON), що можуть включати текст, метадані та мультимедійний вміст. Великі файли часто передаються через CDN-інфраструктуру [5].

У контексті офлайн-повідомлень месенджери зберігають дані протягом визначеного часу (наприклад, 30 днів у Telegram), після чого інформація може бути видалена із серверів відповідно до політик конфіденційності.

Безпека комунікацій є ключовою умовою функціонування месенджерів, оскільки вони опрацьовують персональні та службові дані. Переважна більшість сучасних платформ застосовує наскрізне шифрування (End-to-End Encryption, E2EE), що гарантує доступ до вмісту лише учасникам діалогу. WhatsApp і Signal реалізують E2EE за замовчуванням, використовуючи криптографічні бібліотеки Open Whisper Systems [4]. Telegram застосовує E2EE виключно в «секретних чатах», тоді як звичайні повідомлення шифруються між клієнтом і сервером [3].

Окрім шифрування, значну роль відіграють моделі автентифікації, які можуть включати номери телефонів, PIN-коди або біометричні параметри. Різні платформи по-різному поводяться з метаданими: Signal мінімізує їх збирання, тоді як WhatsApp обробляє їх у межах політик материнської компанії Meta [6].

У сфері цивільного захисту, зокрема в системі ДСНС України, питання конфіденційності набуває особливого значення, оскільки обробляється інформація оперативного характеру. Рекомендованими є платформи з наскрізним шифруванням, а також рішення, які

відповідають чинним вимогам законодавства України у галузі кібербезпеки, зокрема Закону № 2163-VIII [7,8].

Сучасні месенджери виходять за межі функцій текстового обміну й надають можливість створення групових чатів, здійснення голосових та відеодзвінків, використання інтегрованих сервісів і бот-платформ. Telegram надає можливість створення інформаційних каналів та автоматизованих ботів, WhatsApp інтегрується з бізнес-орієнтованими системами, а Signal зосереджується на мінімізації даних і захисті приватності.

Подальший розвиток месенджерів пов'язаний з інтеграцією інструментів штучного інтелекту, удосконаленням аналізу мультимедійних даних та децентралізацією інфраструктури. Разом із цим зростають вимоги до обчислювальних ресурсів, підвищується обсяг даних, а також збільшується кількість загроз, пов'язаних із поширенням дезінформації.

Протягом 2024–2025 років виявлено низку уразливостей у WhatsApp, зокрема CVE-2025-30401, що стосувалася некоректного розпізнавання вкладених файлів у десктопній версії застосунку. Уразливість дозволяла ініціювати виконання некоректно класифікованих вкладень, що створювало потенційні ризики для користувачів. Після публікації проблеми компанія Meta випустила відповідне оновлення безпеки.

Також зафіксовано уразливість CVE-2025-30259, пов'язану з обробкою певних форматів PDF-файлів серверами WhatsApp, що могло дозволяти сторонні впливи на роботу клієнтських застосунків. Наприкінці 2024 року повідомлялося про використання окремими шпигунськими угрупованнями моделей атак типу «zero-click», спрямованих на автоматичне використання вразливостей без взаємодії користувача. Усі виявлені вектори були усунені через оновлення механізмів обробки даних.

На початку 2024 року також описано ситуацію з некоректною обробкою окремих видів вкладених файлів у десктопному клієнті для Windows, що могло створювати ризики автоматичного виконання стороннього коду за наявності відповідного середовища інтерпретації.

Методи компрометації та засоби протидії. Зловмисники використовують широкий спектр технічних і соціальних методів компрометації акаунтів WhatsApp, серед яких – фішинг, підміна SIM-карт, шпигунське програмне забезпечення та використання залежностей у моделі передачі кодів підтвердження. Одним із найпоширеніших методів фішингу є отримання одноразових кодів

підтвердження шляхом соціальної маніпуляції. У випадку підміни SIM-карт атака ґрунтується на отриманні контролю над номером користувача через оператора мобільного зв'язку, що дозволяє відновлювати доступ до акаунта.

Загрозу становлять і атаки, пов'язані з обробкою вкладених файлів, а також моделі компрометації сесій, що передбачають маніпуляцію QR-кодами авторизації або використання шкідливих програм для зчитування натискань клавіш.

Приклад рішення: двофакторна автентифікація (2FA). Двофакторна автентифікація у WhatsApp виступає додатковим механізмом захисту, який істотно підвищує стійкість облікових записів до несанкціонованого доступу. Захист реалізується через введення додаткового PIN-коду, що потрібен під час повторної реєстрації номера або входу з нового пристрою. Завдяки цьому навіть у разі компрометації одноразових SMS-кодів стороння особа не може активувати обліковий запис без знання PIN-коду.

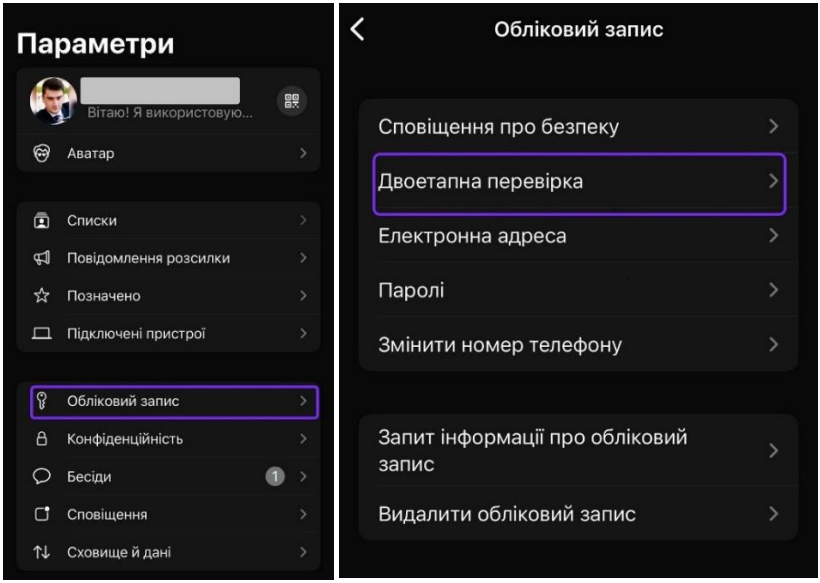

Рис. 3 – Скріншот двофакторної автентифікації WhatsApp

Механізм передбачає періодичне нагадування користувачу про введення PIN-коду для підтримання його актуальності, а також можливість використання електронної пошти як резервного засобу відновлення доступу. Загалом використання 2FA мінімізує ризики, пов'язані з крадіжкою пристрою, підміною SIM-карт та іншими моделями атак, спрямованих на захоплення акаунтів.

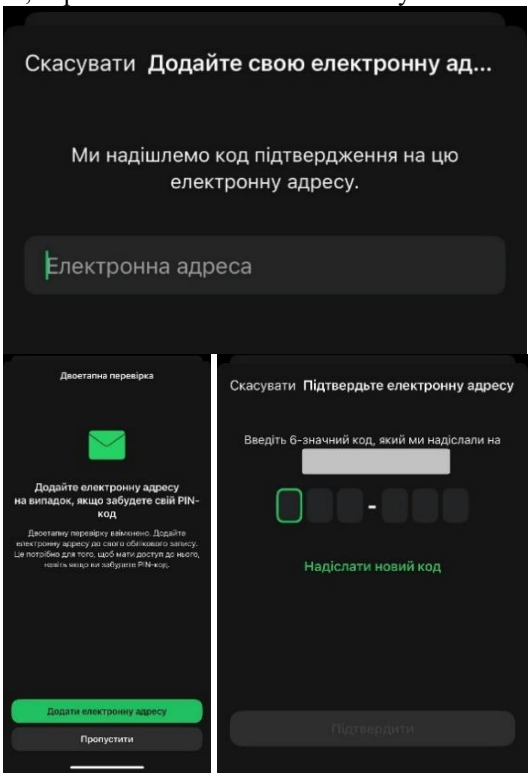

Рис. 4 – Скріншот двофакторної автентифікації WhatsApp

Якщо двофакторна автентифікація не увімкнена, існує значний ризик, що зловмисник може активувати WhatsApp на іншому пристрої, маючи лише доступ до SIM-карти. При цьому користувач не отримає повідомлення про несанкціоновані спроби входу, а у разі втрати або крадіжки телефону акаунт стає легкою мішенню для зловмисників. З огляду на частоту цифрових атак, високу цінність особистих даних і

важливість захисту комунікацій, увімкнення 2FA у WhatsApp є критично необхідним кроком для кожного відповідального користувача. Цей простий, але ефективний інструмент дозволяє запобігти викраденню облікового запису, знизити ризик доступу сторонніх до персональних даних і забезпечити загальну безпеку цифрової ідентичності користувача. Таким чином, застосування двофакторної автентифікації у WhatsApp значно підвищує безпеку особистих даних користувачів, захищаючи їх від поширених сценаріїв несанкціонованого доступу.

Висновки та практичне застосування засобів захисту під час виїзду пожежного автомобіля з оперативним розрахунком. Останнім часом фіксуються небезпечні випадки, коли після первинної повітряної атаки підрозділи пожежно-рятувальної служби оперативно виїжджали на місце події, а згодом по тій самій локації здійснювався повторний удар. Подібна тактика противника спрямована на ураження особового складу, який прибуває для ліквідації наслідків першого обстрілу, що значно підвищує ризики для рятувальників і ускладнює виконання оперативних завдань. З огляду на це, особливого значення набуває максимально можливе обмеження поширення інформації про маршрут, час реагування та склад оперативного розрахунку, а також упровадження технологічних і організаційних заходів, які унеможливлюють використання цієї інформації зловмисниками для повторних або коригованих ударів.

Враховуючи специфіку оперативної роботи рятувальників, ефективне використання захищених месенджерів дозволяє мінімізувати ризики витоку інформації про час, місце та склад пожежних виїздів, що підвищує безпеку персоналу та оперативну ефективність під час ліквідації надзвичайних ситуацій. У контексті оперативної діяльності пожежно-рятувальних підрозділів, де критично важливими є швидкість реагування, точність координації та збереження конфіденційності оперативної інформації, застосування месенджерів повинно здійснюватися з дотриманням заходів кібербезпеки, підтверджених результатами проведеного дослідження. Під час виїзду пожежного автомобіля з оперативним розрахунком передаються важливі дані: адреса події, час прибуття, наявна загроза, чисельність особового складу, тип залученої техніки та інші елементи службової інформації, які можуть бути використані зловмисниками для прогнозування маршрутів руху, коригування вогневих ударів, створення перешкод або дезінформації.

Застосування захищених месенджерів із підтримкою наскрізного шифрування (E2EE), з урахуванням встановленої у ході дослідження стійкості платформ, дозволяє мінімізувати ризик перехоплення або модифікації цих даних. Наприклад, використання Signal або інших платформ із перевіреною криптографічною архітектурою знижує ймовірність несанкціонованого доступу навіть у разі компрометації мережі зв'язку, зокрема при передачі даних через незахищені або тимчасові канали мобільного інтернету.

Активація двофакторної автентифікації (рисунки 3,4) для облікових записів, що застосовуються особами чергової зміни та керівництвом караулу, запобігає можливості захоплення акаунтів через фішингові або SIM-підміни, які згідно з результатами експериментального моделювання становлять один із найпоширеніших векторів атак. Це гарантує, що жоден сторонній суб'єкт не зможе отримати доступ до службових чатів із інформацією про оперативний виїзд навіть у разі перехоплення SMS-кодів або QR-кодів синхронізації.

Урахування виявлених уразливостей у десктопних клієнтах, зокрема типу CVE-2025-30401 для WhatsApp, визначає необхідність застосування лише оновлених месенджерів на службових планшетах, що використовуються диспетчерськими пунктами або оперативними штабами. Це знижує ризик виконання шкідливого коду при відкритті вкладених файлів, які можуть бути замасковані під службові документи, фотографії чи PDF-інструкції.

Також критично важливим є дотримання нормативних документів ДСНС України щодо обмеження використання комерційних месенджерів для передачі інформації, яка може становити загрозу безпеці особового складу або виконання оперативних завдань. У разі необхідності використання месенджерів підрозділи повинні застосовувати лише дозволені канали та алгоритми передавання інформації, що не містять координат, маршрутів або іншої оперативної деталізації, яка може бути однозначно інтерпретована.

Таким чином, упровадження зазначених заходів – використання платформ із E2EE, активація 2FA, уникнення ризикових механізмів синхронізації, застосування оновлених клієнтів і дотримання організаційних норм – дозволяє підвищити кіберстійкість процесу координації під час виїзду пожежно-рятувального підрозділу. Це забезпечує захист службової інформації та знижує ризик її використання зловмисниками для створення загроз оперативному розрахунку або порушення безперервності рятувальних заходів.

Бібліографічні посилання

1. **Rescorla E.** SSL and TLS: Designing and Building Secure Systems / E. Rescorla. – Addison-Wesley, 2001. – 400 с.

2. **Ghernaouti-Hélie S.** Cybersecurity and Cyberwarfare: A Reference Handbook / S. Ghernaouti-Hélie. – ITU, 2013. – 350 с.

3. Telegram. MTProto 2.0: Protocol Specification / Telegram. – 2023.

4. **Marlinspike M., Perrin T.** The Signal Protocol / M. Marlinspike, T. Perrin. – Open Whisper Systems, 2016. – 50 с.

5. **Akamai Technologies.** Content Delivery Networks: Architecture and Performance / Akamai Technologies. – White Paper, 2022. – 28 с.

6. **Meta (Facebook Inc.).** WhatsApp Privacy Policy / Meta Platforms. – 2023.

7. Закон України №2163 VIII Про основні засади забезпечення кібербезпеки України: від 05.10.2017. – Відомості Верховної Ради України, 2017, №77, ст. 2761.

8. Про затвердження Статуту дій у надзвичайних ситуаціях та Статуту з організації внутрішньої, гарнізонної та караульної служб у підрозділах оперативно-рятувальної служби цивільного захисту: Наказ МВС України від 14.06.2021 № 453.

Надійшла до редколегії 25.12.2025