ЗВП 6-00(108).01

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

“З ПИТАНЬ ЗАБЕЗПЕЧЕННЯ ОСОБИСТОЇ КІБЕРБЕЗПЕКИ ВІЙСЬКОВОСЛУЖБОВЦЯ”

СЕРПЕНЬ 2023

Ця військова публікація є першим виданням.

КОМАНДУВАННЯ ВІЙСЬК ЗВ’ЯЗКУ ТА КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Прим. №__

ЗВП 6-00(108).01

ЗАТВЕРДЖЕНО
Наказ Командувача Військ
зв’язку та кібербезпеки
Збройних Сил України
“16” серпня 2023 № 200нагд

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

“З ПИТАНЬ ЗАБЕЗПЕЧЕННЯ ОСОБИСТОЇ КІБЕРБЕЗПЕКИ ВІЙСЬКОВОСЛУЖБОВЦЯ”

Військова навчально-методична публікація військовослужбовцям Збройних Сил України з питань забезпечення кібербезпеки

СЕРПЕНЬ 2023

КОМАНДУВАННЯ ВІЙСЬК ЗВ’ЯЗКУ ТА КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

ПЕРЕДМОВА

Військова навчально-методична публікація “Методичні рекомендації “З питань забезпечення особистої кібербезпеки військовослужбовця” (далі – Методичні рекомендації) розроблені Командуванням Військ зв’язку та кібербезпеки Збройних Сил України спільно з Головним об’єднаним центром захисту інформації та кібербезпеки інформаційно-телекомунікаційних систем ЗС України, Військовим коледжем сержантського складу Військового інституту телекомунікацій та інформатизації імені Героїв Крут та погоджені з Головним управлінням доктрин та підготовки Генерального штабу ЗС України.

Ці Методичні рекомендації визначають порядок організації заходів з кібербезпеки, яка є однією з складових функції генерації Військ зв’язку та кібербезпеки ЗС України, та включають основні правила з налаштування додатків/застосунків, програмного забезпечення, набору інструментів щодо захисту девайсів під управлінням операційних систем Android та iOS, безпеки спілкування у месенджерах та соціальних мережах Signal, Telegram, Viber, WhatsApp, Facebook Messenger, TikTok та налаштування безпеки в браузерах Google Chrome та Microsoft Edge, безпечного користування безпроводовими мережами (Wi-Fi).

Склад робочої групи авторського колективу: полковник **Валентин ДОКІЛЬ** (керівник розроблення), полковник **Юрій КИСИЛЕНКО**, полковник запасу **Євген ЖИВИЛО**, кандидат наук з державного управління, підполковник **Юрій БОНДАРЕНКО**, підполковник **Максим КРАСНОЩОК**, підполковник **Костянтин КРАВЧЕНКО**.

У цих Методичних рекомендаціях використано публікації з кібербезпеки Агентства національної безпеки Сполучених Штатів Америки U/OO/155488-20, PP-20-0622, October 2020 Info Sheet: “Mobile device best practices (Мобільні пристрої – найкращі практики захисту, видання жовтень 2020)” (посилання **л**), U/OO/166417-21, PP-21-1031, July 2021 “CSI: Securing wireless devices in Public Settings (Інформаційний аркуш з кібербезпеки: Захист безпровідних пристроїв при роботі в громадських місцях, видання липень 2021)” (посилання **м**), U/OO/119184-23, PP-23-0270, February 2023 “CSI: Best practices for securing your home network (Інформаційний аркуш з кібербезпеки: Найкращі практики для безпеки вашої домашньої мережі, видання лютий 2023)” (посилання **н**), та з інших відкритих джерел.

Усі питання, що стосуються цих Методичних рекомендацій, надсилати за такими адресами:

03168, м. Київ, Повітрофлотський проспект, 6, Командування Військ зв’язку та кібербезпеки ЗС України; E-mail: css_command_afua@post.mil.gov.ua та “СЕДО М” – індекс 308 (контактний телефон для надання зауважень та пропозицій – (62) 35-279).

ЗМІСТ

“У найбільшій безпеці той, хто напоготові, навіть коли немає небезпеки”.

ВСТУП

З появою сучасних девайсів функціонал їх значно розширився, з’явилися нові можливості – геолокація, месенджери, фільми, ігри тощо. Водночас зазначений функціонал є найпростішим джерелом добування розвідувальної інформації. Новітні засоби розвідки дають змогу дізнатися не лише про місце, з якого ведуться розмови, а й безпосередньо про їх зміст та листування.

Головною проблемою в цьому питанні є недостатній рівень обізнаності особового складу в питаннях забезпечення особистої кібербезпеки під час використання девайсів для ведення розмов та використання сучасних функцій.

Сьогодні більшість з тих, хто залучений до складу сил безпеки і оборони України, не в повному обсязі розуміють існуючі кіберзагрози та потенційно можливі негативні наслідки, які можуть створити небезпеку життєво важливим інтересам громадян, суспільства і держави в цілому під час користування особистими девайсами.

В умовах сьогодення головним обов’язком кожного громадянина є:

забезпечити цілісність і конфіденційність інформації під час виконання бойових завдань у пунктах постійної дислокації, на пунктах управління, у районах зосередження, бойового злагодження, в районах виконання бойових завдань тощо;

усвідомлювати особисту відповідальність за ведення розмов (листування) службового характеру з використанням персональних девайсів та електронних комунікаційних мереж.

На жаль, не всі військовослужбовці в змозі самостійно забезпечити безпечне налагодження та експлуатацію тих чи інших додатків/застосунків, програмного забезпечення, набору інструментів, технологій та захистити особисті (службові) дані від несанкціонованого доступу. До особистого девайса слід ставитися як до засобу, через який ворог збирає (прослуховує) про вас інформацію. З точки зору безпеки краще було б узагалі ВІДМОВИТИСЯ від використання девайсів під час виконання бойових завдань.

Водночас неможливо собі уявити життя без сучасних девайсів. Отже, для збереження життя на полі бою необхідно знати і дотримуватися певних вимог і правил користування девайсами та відповідним програмним забезпеченням.

Отже ці Методичні рекомендації розроблені з метою допомогти військовослужбовцям з питань основних правил особистої кібербезпеки та мають рекомендаційну спрямованість для їх впровадження.

“– Значить, ми знову в безпеці? – В безпеці? Звичайно, ні! Там ще маса всякого, готового знищити ваш світ. Але! Якщо хочете прикинутися, що ви в безпеці тільки, щоб спати по ночах, то так, ви в безпеці, але це не зовсім так”.

1. ПРАВИЛА КІБЕРЗАХИСТУ СМАРТФОНІВ

Порядок зберігання і користування особистими фотоапаратами, магнітофонами, радіоприймачами, мобільними телефонами, іншими засобами мобільного зв’язку та передачі інформації, комп’ютерною та іншою побутовою радіоелектронною технікою для військовослужбовців, які виконують обов’язки військової служби, встановлюється командиром військової частини (посилання **г**, стаття 143). Також, варто користуватися “Інструкцією зі зберігання і користування особовим складом ЗС України засобами стільникового зв’язку та іншими електронними засобами” [3].

Перелік основних рекомендацій, які необхідно виконувати під час користування девайсом:

використовуйте його як засіб для спілкування й Інтернету лише за нагальної потреби;

вимикайте девайс повністю або вмикайте “режим польоту”, коли перебуваєте у безпосередній близькості до позицій ворога або є можливість виявлення ворогом вашого місцезнаходження, коли ви перебуваєте у складі якогось підрозділу, пункту управління тощо;

потурбуйтеся, щоб дані з вашого девайса не потрапили до рук ворога;

використовуйте лише мінімально необхідний набір додатків/застосунків (програмного забезпечення);

використовуйте VPN-технологію, яка шифрує інтернет-трафік і приховує вашу IP-адресу і фізичне розташування;

налаштуйте девайс та встановлені месенджери так, щоб приймати дзвінки та повідомлення лише від осіб зі списку контактів;

не підключайте девайс до комп’ютерів (ноутбуків) військового призначення, Wi-Fi мереж та мобільного Інтернету. Ні в якому разі не підключайтеся до невідомого/сумнівного/підозрілого походження Wi-Fi мереж або інших пристроїв, які надають доступ до мережі Інтернет;

не зберігайте на девайсі фото, відеоматеріали, документи та будь-яку іншу інформацію, яка може бути використана противником у випадку втрати власником свого девайса;

не обговорюйте (не пишіть, не пересилайте) по девайсу, навіть із близькими, будь-яку службову інформацію;

не варто користуватися девайсами одночасно групі (кільком) військовослужбовців(ям) у районі виконання завдань (позиції чи іншого важливого об’єкта). Постійно аналізуйте ситуацію, змінюйте місце (точку) дзвінка, телефонуйте по черзі з певними часовими проміжками, пристосовуйтеся до обставин. Безпечніше дзвонити з місць, віддалених від розташування позицій.

Здійсніть у девайсі такі налаштування безпеки:

обов'язково встановіть блокування девайса. Це може бути PIN-код, пароль, графічний ключ, відбиток пальця, ідентифікація по обличчю, а краще – кілька способів одночасно;

налаштовуйте всюди, де можливо, двофакторну (двоетапну) автентифікацію (процедура встановлення належності істинного користувача);

видаліть непотрібні мобільні додатки/застосунки;

перевірте, які дозволи надані вашим мобільним додаткам/застосункам, змініть їх за необхідності (забороніть доступ до контактів, фото, особистих файлів (інформації);

відмовтеся від функцій автоматичного входу в будь-які акаунти – безпечніше авторизуватися щоразу, коли це необхідно;

забороніть доступ до геолокації;

вимкніть функцію автоматичного вибору мережі (ця опція встановлена в налаштуваннях девайса).

Зазначені в цих Методичних рекомендаціях назви пунктів меню налаштувань девайсів можуть несуттєво відрізнятися залежно від виробника пристрою та типу (версії) операційної системи, що використовується. Якщо ви не знайшли саме вказаний пункт меню, то шукайте пункт з подібною назвою.

2. НАЛАШТУВАННЯ ЗАХИСТУ СМАРТФОНА ПІД УПРАВЛІННЯМ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

2.1. Встановлення пароля на розблокування екрана

Для захисту девайса від зловмисників необхідно встановлювати пароль на розблокування екрана. Операційна система Android дає змогу налаштувати різні способи розблокування екрану: **"ПРОВЕСТИ ПО ЕКРАНУ"**, "**КЛЮЧ", "PIN"** та **"ПАРОЛЬ"**. З них найбільш безпечним є **"ПАРОЛЬ"**.

Використовувати необхідно стійкі паролі довжиною не менше 12 символів, які містять великі й малі літери, цифри та спеціальні символи (наприклад: qSr@17&FDw18).

Для встановлення або зміни пароля на вхід у девайс під управлінням операційної системи Android необхідно:

зайти в **"НАЛАШТУВАННЯ"** девайса;

вибрати пункт **"БЕЗПЕКА ТА МІСЦЕЗНАХОДЖЕННЯ"** (може також називатися **"БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ"** або просто **"БЕЗПЕКА"** тощо);

далі – пункт **"БЛОКУВАННЯ ЕКРАНА"**. У вибраному пункті обираємо **"СКЛАДНИЙ ПАРОЛЬ"** (може також називатися **"ПАРОЛЬ"**), після чого необхідно ввести обраний пароль, потім ще раз підтвердити обраний вами пароль.

2.2. Встановлення сканера відбитка пальця на розблокування екрана (Touch ID)

Використання відбитка фаланги пальця може мати свої переваги, а саме: обмеження доступу до девайса, додатковий етап проходження автентифікації, оперативність активації екрана девайса, набагато рідше введення свого пароля.

За цих умов, залежно від місця вашого перебування, необхідно враховувати ризик можливого примусового розблокування противником екрана девайса шляхом прикладання вашого пальця.

Налаштування цифрового відбитка на девайсі під операційною системою Android:

зайдіть у **“НАЛАШТУВАННЯ”** девайса (“іконка” у вигляді коліщатка, що з’являється, коли ви проводите по екрану згори донизу, або окрема “іконка” – **“НАЛАШТУВАННЯ”** на робочому екрані);

у **“НАЛАШТУВАННЯХ”** оберіть **“БЕЗПЕКА ТА МІСЦЕЗНАХОДЖЕННЯ”** (може також називатися **“БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ”** або **“БЕЗПЕКА”**), а в ньому – пункт **“ВІДБИТОК ПАЛЬЦЯ”** (може також називатися **“ЦИФРОВИЙ ВІДБИТОК”**);

насамперед система запросить ввести пароль до девайса. Після цього ви побачите екран, на якому вам запропонують прикласти кілька разів палець до сканера відбитків, щоб відсканувати різні частини відбитка. Продовжуйте це робити, поки відбиток не буде повністю просканово.

2.3. Налаштування сповіщень на заблокованому екрані

На заблокованому екрані девайса під операційною системою Android можуть виводитися сповіщення про нові листи, повідомлення в месенджерах тощо. При цьому, принаймні частково, може з’являтися текст самого повідомлення. Так, будь-хто, хто візьме ваш девайс у руки, може читати ці повідомлення, навіть не знаючи пароля. Тому доречно налаштувати сповіщення так, щоб на заблокованому екрані не показувався їх зміст.

Для налаштування сповіщення на заблокованому екрані девайса під операційною системою Android необхідно:

зайти у **“НАЛАШТУВАННЯ”** девайса;

у **“НАЛАШТУВАННЯХ”** вибрати пункт **“БЕЗПЕКА ТА МІСЦЕЗНАХОДЖЕННЯ”** (може також називатися **“БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ”** або **“БЕЗПЕКА” ЧИ “СПОВІЩЕННЯ”**), а в ньому – пункт **“НАЛАШТУВАННЯ ЗАБЛОКОВАНОГО ЕКРАНА”** (може також називатися **“КОНФІДЕНЦІЙНІ СПОВІЩЕННЯ”**)*;*

обрати пункт **“НА ЗАБЛОКОВАНОМУ ЕКРАНІ”**, а у випадному вікні – **“ХОВАТИ КОНФІДЕНЦІЙНИЙ ВМІСТ”** (може також називатися **“КОНФІДЕНЦІЙНІ СПОВІЩЕННЯ”**).

Тепер зловмисник, який отримає короткочасний доступ до вашого заблокованого девайса, не зможе прочитати зміст сповіщень, що виводяться на екран.

2.4.Налаштування повнодискового шифрування

Якщо противник все ж таки заволодів вашим девайсом та отримав фізичний доступ до нього, одного лише пароля буде недостатньо. У цьому випадку дані та інформацію, які знаходяться на ньому, можна захистити лише за допомогою повнодискового шифрування.

Щоб налаштувати повнодискове шифрування девайса під операційною системою Android, необхідно:

зайти у **“НАЛАШТУВАННЯ”** девайса;

вибрати пункт **“БЕЗПЕКА ТА МІСЦЕЗНАХОДЖЕННЯ”** (**“БЕЗПЕКА”**, **“БІОМЕТРИЧНІ ДАНІ ТА БЕЗПЕКА”** тощо), а в ньому – **“ШИФРУВАННЯ Й ОБЛІКОВІ ДАНІ”**, далі – **“ЗАШИФРУВАТИ ТЕЛЕФОН”** (може також називатися **“ШИФРУВАННЯ”** > **“ШИФРУВАТИ ТЕЛЕФОН”);**

також у меню **“НАЛАШТУВАННЯ”** зазвичай доступний пошук по всіх налаштуваннях девайса, спробуйте ввести туди слово **“ШИФРУВАННЯ”.**

Перед початком шифрування вам буде запропоновано поставити девайс на зарядку і залишити його увімкненим під час процесу шифрування.

ЗАСТЕРЕЖЕННЯ! Оскільки шифрування є складною процедурою, існує невеликий, але ненульовий ризик втрати важливих даних на девайсі в процесі шифрування. Тому перед початком шифрування обов’язково створіть резервну копію всіх важливих даних!

2.5. Перевірка оновлень операційної системи

Час від часу в будь-якому програмному забезпеченні, включаючи операційні системи, виявляються вразливості, які можуть бути використані зловмисниками. Тому розробники програмного забезпечення регулярно випускають оновлення, включаючи оновлення безпеки, які виправляють відомі вразливості. Без своєчасних оновлень ваш пристрій стає більш вразливим.

Для перевірки оновлень програмного забезпечення девайса під операційною системою Android необхідно:

зайти у **“НАЛАШТУВАННЯ”;**

знайти пункт **“БЕЗПЕКА ТА МІСЦЕЗНАХОДЖЕННЯ”** (може також називатися **“БЕЗПЕКА”**), а в ньому – **“ОНОВЛЕННЯ СИСТЕМИ БЕЗПЕКИ”;**

для перевірки наявності оновлень натисніть **“ШУКАТИ ОНОВЛЕННЯ”**.

Якщо ви хочете впевнитися/дізнатися, чи отримав ваш пристрій останнє оновлення системи безпеки, ви можете порівняти дату останнього встановленого оновлення з датою останнього оновлення, випущеного на офіційному вебсайті Android за посиланням https://www.android.com.

2.6. Налаштування резервної копії

Операційна система Android дозволяє налаштувати резервне копіювання вашого девайса, включаючи дані додатків/застосунків, історію дзвінків, контакти, налаштування пристрою та SMS. За необхідності ці дані можна відновити на новому девайсі. Однак необхідно зауважити, що резервна копія зберігається у вашому обліковому записі Google і вона має бути належним чином захищена.

Налаштування резервної копії девайса під операційною системою Android здійснюється таким чином:

зайдіть у **“НАЛАШТУВАННЯ”**;

далі – **“СИСТЕМА”,** а в ній – **“РЕЗЕРВНЕ КОПІЮВАННЯ”** (може також називатися **“РЕЗЕРВНЕ КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ ДАНИХ”**);

щоб увімкнути резервне копіювання, натисніть **“ЗАВАНТАЖУВАТИ НА GOOGLE ДИСК”**.

3. НАЛАШТУВАННЯ ЗАХИСТУ СМАРТФОНА ПІД УПРАВЛІННЯМ ОПЕРАЦІЙНОЇ СИСТЕМИ iOS

3.1. Встановлення пароля на розблокування екрана

У нових версіях девайсів Apple для розблокування екрана можна встановити чотиризначний чи шестизначний PIN-код, або парольну фразу будь-якої довжини, Touch ID або Face ID.

Для встановлення або зміни пароля на вхід у девайс під управлінням операційної системи iOS необхідно:

відкрити меню **“ПАРАМЕТРИ”**;

прогорнути вниз, знайти та натиснути **“TOUCH ID”** і код допуску;

якщо на девайсі вже встановлено пароль, операційна система iOS спершу запросить його ввести. У новому вікні натисніть **“ВСТАНОВИТИ КОД ДОПУСКУ”** (у разі відсутності раніше встановленого пароля) або **“ЗМІНИТИ КОД ДОПУСКУ”**;

при зміні коду допуску можна змінити його параметри, обравши **“ОПЦІЇ КОДУ ДОПУСКУ”,** а саме обрати 4/6-значний числовий код або парольну фразу довільної довжини;

введіть та підтвердіть новий код допуску.

3.2. Встановлення сканера відбитка пальця на розблокування екрана (Touch ID та Face ID). Встановлення пароля на додатки/застосунки

Умови використання Touch ID девайсів Apple під операційною системою iOS у цілому відповідають таким же умовам використання, як і в девайсах під операційною системою Android.

3.2.1. Налаштування цифрового відбитка – Touch ID:

відкрийте меню **“ПАРАМЕТРИ”**;

прогорніть вниз, знайдіть та натисніть ***“TOUCH ID”*** і код допуску. Операційна система iOS запросить ввести пароль;

натисніть **“ДОДАТИ ВІДБИТОК”**. Стежте за вказівками на екрані та прикладайте фалангу пальця до сенсора.

Після успішного додавання одного відбитка рекомендується додати ще один відбиток на випадок травми, наприклад, порізу пальця.

3.2.2. Налаштування сканера об’ємно-просторової форми обличчя людини – Face ID

Face ID – це один із способів автентифікації шляхом розпізнавання обличчя. Сканер Face ID дозволяє запобігти небажаному розблокуванню девайсів Apple, надавати доступ до певних програм, папок, інформації або даних, а також авторизувати покупки.

Налаштування сканера об’ємно-просторової форми обличчя людини девайсів Apple під операційною системою iOS:

зайдіть у **“ПАРАМЕТРИ”** девайса та оберіть опцію **“FACE ID І КОД ДОПУСКУ”**. Якщо потрібно, введіть код допуску. Якщо ви не встановили код допуску, вам буде запропоновано його створити, щоб використовувати як альтернативний спосіб перевірки вашої особи;

тримаючи девайс у портретній орієнтації, розташуйте його перед своїм обличчям і оберіть **“ПОЧАТИ”;**

розташуйте девайс так, щоб обличчя опинилося в рамці, і плавно рухайте головою, щоб обвести повне коло. Якщо ви не можете рухати головою, виберіть пункт **“ОПЦІЇ ДОСТУПНОСТІ”**;

після того, як перше сканування Face ID завершиться, натисніть **“ПРОДОВЖИТИ”**;

плавно рухайте головою, щоб обвести повне коло вдруге;

натисніть **“ГОТОВО”;**

щоб вибрати функції, які ви хочете використовувати з Face ID або скинути Face ID, перейдіть до меню **“ПАРАМЕТРИ”**, а потім торкніться пункту **“FACE ID І КОД ДОПУСКУ”**;

відкрийте меню **“ПАРАМЕТРИ”**, а потім торкніться пункту **“FACE ID І КОД ДОПУСКУ”**. Якщо потрібно, введіть код допуску.

3.2.3. Встановлення пароля на додатки/застосунки

Для більшої безпеки необхідно встановити паролі на додатки/застосунки, які зберігають приватну інформацію (галерея, месенджери, соціальні мережі тощо):

активуйте функцію **“ЕКРАННИЙ ЧАС”** у відповідному підпункті меню **“ПАРАМЕТРИ”**;

натисніть на сенсорну кнопку **“ВИКОРИСТОВУВАТИ КОД-ПАРОЛЬ”** і введіть будь-яку відому лише вам послідовність символів;

торкніться **“ГРАФІКА СТАТИСТИКИ ВИКОРИСТАННЯ ПРОГРАМ”** на вашому девайсі та оберіть потрібну програму зі списку;

у самому низу екрана розташовуватиметься опція з написом **“ДОДАТИ ЛІМІТ”**. Необхідно її натиснути та встановити час, наприклад, 1 хвилина. Після цього достатньо активувати опцію навпроти параметра **“БЛОКУВАТИ”** в кінці списку.

Після закінчення встановленого часу (у прикладі однієї хвилини) програма заблокується. Для її розблокування достатньо натиснути на кнопку **“ІГНОРУВАТИ ЛІМІТ”** і ввести обраний при налаштуванні пароль.

3.3. Налаштування сповіщень на заблокованому екрані

Для налаштування сповіщення на заблокованому екрані девайсів Apple під операційною системою iOS необхідно:

відкрити меню **“ПАРАМЕТРИ”**;

знайти та обрати опцію **“СПОВІЩЕННЯ”**;

обрати **“ПЕРЕДОГЛЯД”**, далі – **“КОЛИ ВІДІМКНЕНО”**, що приховуватиме вміст усіх повідомлень з усіх програм на заблокованому екрані пристрою.

Після проведення необхідних налаштувань, з метою перевірки відповідних маніпуляцій, попросіть когось надіслати вам повідомлення та перевірте, що видно на заблокованому екрані пристрою.

3.4. Налаштування повнодискового шифрування

Виробники девайсів Apple з операційною системою iOS (починаючи з iPhone 4s) реалізували декілька корисних нововведень, пов’язаних з організацією та управлінням паролями. Це означає, що якщо на вашому пристрої встановлений надійний пароль, відомий тільки вам, противник/зловмисник не зможе отримати доступ до інформації на вашому пристрої в разі крадіжки або його вилучення.

На практиці краще використовувати останні моделі, які мають краще апаратне забезпечення.

3.5. Перевірка оновлень операційної системи

Автоматичне оновлення програмного забезпечення девайсів Apple з операційною системою iOS здійснюється таким чином:

відкрийте меню **“ПАРАМЕТРИ”**;

знайдіть і натисніть опцію **“ЗАГАЛЬНІ”**;

натисніть **“ОНОВЛЕННЯ ПЗ”**;

натисніть **“АВТООНОВЛЕННЯ”**. Це дозволить в автоматичному режимі встановити останню версію функцій та безпеки операційної системи iOS.

За умови, що на платформі розробника (App Store) вже є нове оновлення, переконайтеся, що пристрій заряджений щонайменше на 75% (підключіть його до джерела живлення) і під’єднайтеся до швидкого Wi-Fi з’єднання, а потім натисніть **“ЗАВАНТАЖИТИ ТА ВСТАНОВИТИ”**. Автоматично буде запропоновано ввести код доступу.

3.6. Налаштування резервної копії

Налаштування резервної копії девайсів Apple з операційною системою iOS здійснюється таким чином:

під’єднайте смартфон до швидкого Wi-Fi з’єднання;

зайдіть у **“ПАРАМЕТРИ”**;

оберіть верхній рядок (зі своїм ім’ям) та натисніть на **“ICLOUD”**;

погодьтеся на *“Створити резервну копію”*.

4. ЗАХИСТ СМАРТФОНА ВІД ШПИГУНІВ

4.1. Ознаки зламу смартфона

Є низка непрямих ознак, які можуть свідчити про те, що девайс був зламаний, а саме:

зміна налаштувань без підтвердження власником девайса (головна ознака присутності небажаного програмного забезпечення);

великі обсяги трафіку, що передають деякі додатки/застосунки, навіть якщо ви їх рідко використовуєте (Android дає можливість перевірити це в налаштуваннях у розділі **“СТАТИСТИКА ВИКОРИСТАННЯ МОБІЛЬНОГО ТРАФІКУ”**; у iOS необхідно зайти в **“ПАРАМЕТРИ”** у розділ **“СТІЛЬНИКОВІ ДАНІ”**, де доступний контроль використання трафіку за кожний додаток/застосунок);

автоматичне включення Wi-Fi мереж та мобільного Інтернету або геолокації навіть при відключенні опцій вручну;

швидке розрядження девайса;

несподівані сповіщення і повідомлення, в тому числі про помилки в програмному забезпеченні.

4.2. Захист від шпигунського програмного забезпечення

Для захисту від шпигунського програмного забезпечення завжди корисно застосовувати регулярні запобіжні заходи. Разової перевірки може бути недостатньо. Зокрема це стосується завчасного копіювання важливих даних, таких як контакти, та повного "скидання" налаштувань девайса.

Також потрібно постійно пам'ятати про базові правила кібергігієни, які убезпечать вас від більшості загроз в Інтернеті, а саме:

регулярно перевіряти, які додатки/застосунки на девайсі мають доступ до персональних даних;

встановлювати програмне забезпечення тільки з перевірених та достовірних джерел (магазинів App Store і Google Play, офіційних сайтів розробників);

використовувати двофакторну автентифікацію всюди, де вона передбачена розробником;

використовувати ліцензійне антивірусне програмне забезпечення;

регулярно перевіряти, чи не скомпрометовані паролі, і за потреби їх змінювати;

не переходити за посиланнями від невідомих відправників у месенджерах та соціальних мережах;

використовувати екранний пароль на девайс;

для девайсів на Android потрібно купувати мобільні пристрої відомих виробників, які були легально ввезені в Україну, щоб уникнути шпигунських програм, які можуть бути вбудовані виробниками у девайси.

Додаткові рекомендації наведено в додатку 1 до цих Методичних рекомендацій.

5. НАЛАШТУВАННЯ БЕЗПЕКИ СПІЛКУВАННЯ У ПОПУЛЯРНИХ МЕСЕНДЖЕРАХ ТА СОЦІАЛЬНИХ МЕРЕЖАХ

5.1. Порядок активації двофакторної автентифікації у месенджерах Signal, Telegram, Viber, WhatsApp, Facebook Messenger

У наш час найпоширенішими месенджерами є Signal, Telegram, Viber, WhatsApp, Facebook Messenger. Використання двофакторної автентифікації допоможе уберегти себе від перехоплення зловмисником контролю над вашим обліковим записом. Нижче наведено порядок активації двофакторної автентифікації, а також загрози використання певних додатків.

5.1.1. Захист у месенджері Signal

Налаштування двофакторної автентифікації у месенджері Signal.

Відкрийте додаток/застосунок месенджер Signal > натисніть "іконку" профілю у лівому верхньому куті > перейдіть у **"НАЛАШТУВАННЯ"** > натисніть **"ОБЛІКОВИЙ ЗАПИС"** > **"PIN SIGNAL"** > оберіть **"СТВОРІТЬ PIN-КОД"** > введіть PIN-код двічі > натисніть **"ОБЛІКОВИЙ ЗАПИС"** >

“PIN SIGNAL” > увімкніть **“БЛОКУВАННЯ ДОСТУПУ”** – блокування реєстрації. При повторній авторизації у месенджері Signal з цього номера обов’язково буде потрібно вказати PIN-код.

Месенджер Signal дозволяє використовувати пароль (наприклад, комбінацію букв і цифр) замість цифрового PIN-коду. Для цього оберіть **“СТВОРИТИ PIN-КОД”** > натисніть **“СТВОРИТИ БУКВЕНО-ЦИФРОВИЙ PIN-КОД”** > використовуйте різні великі та малі літери, розділові знаки, а також цифри.

Додаткові налаштування безпеки додатка/застосунку месенджера Signal: відкрийте додаток/застосунок месенджер Signal > натисніть “іконку” профілю у лівому верхньому куті > перейдіть у **“НАЛАШТУВАННЯ”** > **“ОБЛІКОВИЙ ЗАПИС”** > **“PIN SIGNAL”** > оберіть **“ЗМІНИТИ PIN-КОД”** > ввімкніть **“НАГАДУВАННЯ PIN-КОДУ”** та **“БЛОКУВАННЯ ДОСТУПУ”** – блокування реєстрації > вихід з **“ОБЛІКОВИЙ ЗАПИС”** > перехід **“ПРИВ’ЯЗАНІ ПРИСТРОЇ”** > відв’яжіть пристрої, якими не користуєтеся > вийдіть з **“ПРИВ’ЯЗАНІ ПРИСТРОЇ”** > оберіть **“ЧАТИ”** > вимкніть **“ВИКОРИСТОВУВАТИ СИСТЕМНІ ФОТО КОНТАКТІВ”** (може також називатися **“ВИКОРИСТОВУЙТЕ ФОТОГРАФІЇ З АДРЕСНОЇ КНИГИ”**) та **“ЗАЛИШАТИ СТИШЕНІ ЧАТИ ЗААРХІВОВАНИМИ”** > вихід з **“ЧАТИ”** > перейдіть до **“КОНФІДЕНЦІЙНІСТЬ”** (може також називатися **“ПРИВАТНІСТЬ”**) > оберіть **“ЗНИКАЮЧІ ПОВІДОМЛЕННЯ”** > оберіть на свій розсуд **“ТАЙМЕР ЗНИКНЕННЯ ПОВІДОМЛЕНЬ”** (може також називатися **“ТАЙМЕР ЗА УМОВЧАННЯМ ДЛЯ НОВИХ ЧАТІВ”**) > перейдіть до **“КОНФІДЕНЦІЙНІСТЬ”** (може також називатися **“ПРИВАТНІСТЬ”**) > **“БЕЗПЕКА ПРОГРАМИ”** > ввімкніть **“БЛОКУВАННЯ ЕКРАНА”** (може також називатися **“БЕЗПЕКА ЕКРАНА”**, **“ПРИХОВУВАТИ ЕКРАН”**) перемикачем застосунку > оберіть **“ПЛАТЕЖІ”** > ввімкніть **“ЗАХИСТ ПЛАТЕЖІВ”**.

5.1.2. Захист у месенджері Viber

Налаштування двофакторної автентифікації у месенджері Viber.

Відкрийте додаток/застосунок месенджер Viber > натисніть у правому нижньому куті **“ДОДАТКОВО”** > **“ПАРАМЕТРИ”** > **“КОНФІДЕНЦІЙНІСТЬ”** > **“ДВОЕТАПНА ПЕРЕВІРКА”** > створіть PIN-код.

Адреса електронної пошти, яку ви раніше використовували для налаштування свого облікового запису/акаунта у месенджері Viber, з’явиться на сторінці підтвердження електронної пошти. Натисніть **“ДАЛІ”**, щоб продовжити і завершити налаштування двофакторної автентифікації. Крім того, якщо ви не налаштували адресу електронної пошти або хочете використовувати іншу адресу електронної пошти, введіть свою адресу електронної пошти. На екрані з’явиться підтвердження налаштування двофакторної автентифікації.

Перевірка інформації, яку бачать інші користувачі про вас:

відкрийте додаток/застосунок месенджер Viber > натисніть у правому нижньому куті **“ДОДАТКОВО”** > **“ПАРАМЕТРИ”** > **“КОНФІДЕНЦІЙНІСТЬ”** та оберіть інформацію, яку ви бажаєте приховати.

5.1.3. Захист у месенджері WhatsApp

Налаштування двофакторної автентифікації у месенджері WhatsApp.

Відкрийте додаток/застосунок месенджер WhatsApp > оберіть **“ПАРАМЕТРИ”/“НАЛАШТУВАННЯ”** > **“ОБЛІКОВИЙ ЗАПИС”** > **“ДВОЕТАПНА ПЕРЕВІРКА”** > натисніть **“УВІМКНУТИ”** > створіть шестизначний пароль. Вам потрібно буде вводити його регулярно і щоразу, коли ви реєструєте месенджер WhatsApp на новому пристрої. Введіть свою електронну адресу на випадок, якщо ви забудете або втратите свій код.

Увімкнення сповіщення безпеки у месенджері WhatsApp.

Відкрийте додаток/застосунок месенджер WhatsApp > оберіть **“ПАРАМЕТРИ”/“НАЛАШТУВАННЯ”** > **“ОБЛІКОВИЙ ЗАПИС”** > **“СПОВІЩЕННЯ ПРО БЕЗПЕКУ”** > **“ПОКАЗАТИ СПОВІЩЕННЯ СИСТЕМИ БЕЗПЕКИ”** (може також називатися **“ПОКАЗАТИ СПОВІЩЕННЯ СИСТЕМИ БЕЗПЕКИ НА ЦЬОМУ ПРИСТРОЇ”**) та встановіть важіль зеленого кольору.

5.1.4. Захист у месенджері Telegram

Налаштування двофакторної автентифікації у месенджері Telegram.

Відкрийте додаток/застосунок месенджер Telegram > натисніть кнопку меню у верхньому лівому куті екрана > оберіть **“НАЛАШТУВАННЯ”** > **“ПРИВАТНІСТЬ І БЕЗПЕКА”** > **“ДВОЕТАПНА ПЕРЕВІРКА”** > введіть пароль.

Увімкнення наскрізного шифрування у месенджері Telegram.

Відкрийте додаток/застосунок Telegram > у нижньому правому куті екрана натисніть значок олівця (новий чат) > оберіть **“НОВИЙ СЕКРЕТНИЙ ЧАТ”** > виберіть контакт, щоб почати секретний чат.

Перевірка інформації, яку бачать інші користувачі про вас.

Відкрийте додаток/застосунок месенджер Telegram > натисніть кнопку меню у верхньому лівому куті екрана > оберіть **“НАЛАШТУВАННЯ”** > **“ПРИВАТНІСТЬ І БЕЗПЕКА”**, в цьому вкладенні можна переглянути та змінити доступ до ваших даних.

Кіберзагрози від використання Telegram-ботів.

Небезпечними можуть бути не тільки мобільні додатки/застосунки, а й Telegram-боти зазначеного додатка/застосунку. Такі Telegram-боти можуть бути запрограмовані на злам облікових записів користувачів, пошук контактної інформації в Інтернеті, розсилку спаму та виконання інших шкідливих дій.

Довідкова інформація, щодо основних типів ботів:

спам-боти – можуть збирати адреси електронної пошти зі сторінок контактів і гостьових книг. Вони також можуть розміщувати рекламний контент на форумах і в коментарях, щоб спрямувати трафік на "підозрілі" сайти;

шкідливі чат-боти – видають себе за живих людей, наслідуючи реальне людське спілкування. Часто їхніми жертвами стають користувачі, які не усвідомили, що спілкуються зі шкідливими програмами, метою яких є отримання особистої інформації, включаючи дані банківських кредитних карток;

боти-обмінники файлів – отримують від користувача запит (наприклад, популярний фільм або музичний альбом), а у відповідь повідомляють, що вони мають доступний для завантаження файл і надають посилання. Користувач переходить за посиланням, завантажує та відкриває його й неусвідомлено заражає свій девайс;

моніторингові боти – використовуються для перевантаження поштових серверів, а також для великомасштабних крадіжок даних.

Щоб запобігти доступу ботів до даних користувачів, необхідно дотримуватися нижченаведених правил безпеки:

увімкніть у месенджері Telegram двоетапну перевірку > перейдіть до **"НАЛАШТУВАННЯ"** > **"ПРИВАТНІСТЬ І БЕЗПЕКА"** > **"ДВОЕТАПНА ПЕРЕВІРКА"** (тоді кожен вхід в акаунт буде супроводжуватися SMS-кодом);

користуйтеся, по можливості, лише офіційними ботами (це ті, в яких є синя відмітка від месенджера Telegram);

ні в якому разі не надсилайте ботам паролі, коди та інші конфіденційні дані.

5.1.5. Захист у соціальній мережі Facebook Messenger

Налаштування двофакторної автентифікації у соціальній мережі Facebook.

Відкрийте додаток/застосунок соціальної мережі Facebook > оберіть **"МЕНЮ"** > натисніть **"НАЛАШТУВАННЯ БЕЗПЕКИ ТА АВТОРИЗАЦІЇ"** (може також називатися **"НАЛАШТУВАННЯ ТА КОНФЕДЕНЦІЙНІСТЬ"**) > **"НАЛАШТУВАННЯ"** > **"ЦЕНТР ОБЛІКОВИХ ЗАПИСІВ"** > **"ПАРОЛЬ І БЕЗПЕКА"** > оберіть розділ **"ВИКОРИСТАТИ ДВОФАКТОРНУ АВТЕНТИФІКАЦІЮ"** (може також називатися **"ДВОЕТАПНА ПЕРЕВІРКА"**) > натисніть **"РЕДАГУВАТИ"** > оберіть потрібний спосіб перевірки > дотримуйтеся інструкцій на екрані.

При налаштуванні двофакторної автентифікації ви зможете обрати один зі способів перевірки:

ключ безпеки на сумісному пристрої;

коди для входу, що генеруються стороннім додатком/застосунком для автентифікації;

SMS-коди, що надходять на мобільний пристрій.

Увімкнення наскрізного шифрування у соціальній мережі Facebook.

Відкрийте додаток/застосунок Facebook > перейдіть до профілю користувача (зазначене можна зробити, обравши **“ЧАТ З КОРИСТУВАЧЕМ”** і натиснувши на його фотографію профілю) > у розділі **“ІНШІ ДІЇ”** виберіть **“ПЕРЕЙТИ ДО СЕКРЕТНОЇ РОЗМОВИ”** > почніть листування.

5.2. Соціальна мережа Instagram як джерело цінних розвідданих

Instagram доцільно вважати джерелом розвідданих, тому що додаток потенційно дає можливість противнику стежити за розміщенням, переміщеннями та кількістю особового складу підрозділу. Тому правильним рішенням є видалення Instagram зі свого девайса. У разі, якщо ви все ж таки не видаляєте його, необхідно виконати такі дії, щоб максимально анонімізувати його та захистити від зламу:

створіть обліковий запис Instagram, який не розкриває вашу особу. Використовуйте додаткову анонімну адресу електронної пошти та видаліть особисту інформацію, де це можливо;

використовуйте вигадані ім’я та дату народження, щоб зменшити ймовірність стати жертвою крадіжки особистих даних;

не прив’язуйте Instagram до своїх акаунтів в інших соціальних мережах, особливо до вашого основного акаунта Facebook – чим більше інформації Instagram може використати для створення вашого профілю, тим більше додаток буде втручатися у ваше приватне життя;

зробіть свій обліковий запис закритим. Для цього натисніть на фігуру людини в нижньому правому куті застосунку Instagram для переходу на сторінку свого профілю > оберіть **“ПАРАМЕТРИ Й КОНФІДЕНЦІЙНІСТЬ”** (може також називатися **“КОНФІДЕНЦІЙНІСТЬ І БЕЗПЕКА”**) > перейдіть **“КОНФІДЕНЦІЙНІСТЬ АКАУНТА”** > ввімкнути **“ЗАКРИТИЙ АКАУНТ”***;*

обмежте дозволи іншим додаткам взаємодіяти з Instagram. Для цього натисніть на фігуру людини в нижньому правому куті застосунку Instagram > оберіть **“ПАРАМЕТРИ Й КОНФІДЕНЦІЙНІСТЬ”** (може також називатися **“КОНФІДЕНЦІЙНІСТЬ І БЕЗПЕКА”**) > перейдіть **“ДОЗВОЛИ САЙТУ”** > перейдіть **“ДОДАТКИ ТА САЙТИ”** > видаліть всі наявні додатки в списку*;*

Налаштуйте двофакторну автентифікацію Instagram.

Налаштування двофакторної автентифікації в Instagram.

Відкрийте додаток/застосунок Instagram > натисніть на фігуру людини, у нижньому правому куті застосунку Instagram для переходу на сторінку свого профілю > оберіть **“ПАРАМЕТРИ Й КОНФІДЕНЦІЙНІСТЬ”** (може також називатися **“КОНФІДЕНЦІЙНІСТЬ І БЕЗПЕКА”**) > перейдіть **“ЦЕНТР ОБЛІКОВИХ ЗАПИСІВ”** > **“ПАРОЛЬ І БЕЗПЕКА”** > оберіть розділ **“ВИКОРИСТАТИ ДВОФАКТОРНУ АВТЕНТИФІКАЦІЮ”** (може також називатися **“ДВОЕТАПНА ПЕРЕВІРКА”***)* > натисніть **“РЕДАГУВАТИ”** > оберіть потрібний спосіб перевірки > дотримуйтеся інструкцій на екрані.

При налаштуванні двофакторної автентифікації ви зможете обрати один із способів перевірки:

ключ безпеки на сумісному пристрої;

коди для входу, що генеруються стороннім додатком/застосунком для автентифікації;

SMS-коди, що надходять на мобільний пристрій;

використовуйте VPN-технологію високого рівня надійності. Instagram може легко отримати доступ до вашого місцезнаходження, використовуючи вашу IP-адресу або GPS. Використання VPN-технології зробить ваше користування Instagram безпечнішим.

5.3. Соціальна мережа TikTok як джерело цінних розвідданих

У світі останніми роками точиться доволі аргументована дискусія щодо заборони урядами низки країн (США, Канада, Індія, Велика Британія, Бельгія, Нова Зеландія) використання додатка/застосунку TikTok на корпоративних пристроях у державних установах.

Нижче наведено неповний список технологій логування і стеження за користувачами, знайдених у додатку/застосунку TikTok:

“Конфігурація смартфона” (до неї входить модель процесора, кількість ядер, унікальні ідентифікатори “заліза”, дозвіл екрана і щільність пікселів на дюйм, обсяг зайнятої оперативної пам’яті, обсяг вільної пам’яті в накопичувачі і т.ін.);

“Список встановлених застосунків” (його збирають, використовуючи спеціальні інструменти, безпосередньо на Android, наприклад: “Працюючий у фоні застосунок TikTok перехоплює відкриття посилань у сторонніх програмах, використовуючи доступ до буфера обміну”, саме в iOS 14 він був ідентифікований);

“Мережеві дані” (побудова з’єднання структури/моделі мережі за описом принципів роботи набору мережевих протоколів, що взаємодіють один з одним, за алгоритмом: локальна IP-адреса > MAC-адреса роутера, назва точки доступу Wi-Fi мережі);

“Наявність рута” (застосунок TikTok ніяк не реагує на ті або інші кіберінциденти, пов’язані з вашим девайсом, але знає, чи “зламаний” ваш девайс, чи ні);

“Геолокація за GPS” (зчитується приблизно 1 раз на 30 секунд. Стеження активується один раз і залишається активним до ручного відключення в системних налаштуваннях девайса з моменту, коли користувач уперше вказав геопозицію поста в TikTok);

“Особисті дані” (це логи SMS-повідомлень, список контактів, історія дзвінків. Мікрофон девайса вмикається навіть тоді, коли користувачеві це непотрібно).

Крім зазначеного, додаток/застосунок має дуже багато “особливостей”. Нижче наведено ті, які вдалося виявити і підтвердити експертам з кібербезпеки:

“Запуск проксі-сервера на пристрої” (передбачається, що він використовується для перекодування медіафайлів, але його справжнє призначення невідоме. Сервер не має жодного захисту чи автентифікації і є справжньою “дірою”);

“Відкритий протокол HTTP для передачі даних” (використовувався донедавна. Дослідники неодноразово демонстрували, як легко викрасти або замінити дані користувачів TikTok, якщо вони мають доступ до тієї ж мережі, що й користувачі TikTok. Можна було навіть замінити відеоматеріали у цій мережі);

“Завантаження будь-якого ZIP-архіву із сервера і запуск виконуваних файлів у ньому” (звісно, підтримується розархівування ZIP-архівів. Сліди коду було знайдено в TikTok для Android. Призначення невідоме. Код також був знайдений у “попередньому” поколінні сервісу, musical.ly, і був добре схований);

“Відключення додатка/застосунку в разі заборони передачі особистих даних” (якщо додаток помітить, що користувач якимось чином блокує з’єднання TikTok із серверами, які отримують персональні дані (наприклад, DNS-фільтр), операцію буде відхилено. Об’єктивних причин для такої відмови немає);

“Відправлення даних” (на 70 різних серверів, понад 30 із яких – китайські).

Беручи до уваги все вищевикладене, можна зробити висновок, що єдиним правильним рішенням є видалення TikTok зі свого девайса. У разі, якщо ви все ж таки не видаляєте його, необхідно виконати наведені нижче дії, щоб максимально анонімізувати його:

створіть обліковий запис TikTok, який не розкриває вашої особи. Використовуйте додаткову анонімну адресу електронної пошти та видаліть особисту інформацію, де це можливо;

використовуйте вигадані ім’я та дату народження, щоб зменшити ймовірність стати жертвою крадіжки особистих даних;

не прив’язуйте TikTok до своїх акаунтів в інших соціальних мережах, бо чим більше інформації TikTok може використати для створення вашого профілю, тим більше цей додаток буде втручатися у ваше приватне життя;

зробіть свій обліковий запис приватним. Щоб налаштувати приватність свого облікового запису, необхідно: натиснути **“НА ТРИ КРАПКИ”**, у верхньому правому куті застосунку TikTok > оберіть **“ПАРАМЕТРИ Й КОНФІДЕНЦІЙНІСТЬ”** (може також називатися **“КОНФІДЕНЦІЙНІСТЬ І БЕЗПЕКА”**) > перейдіть **“КОНФІДЕНЦІЙНІСТЬ”** > **“ВИДИМІСТЬ”** > ввімкнути **“ПРИВАТНИЙ АКАУНТ”***;*

обмежте коло тих, хто може бачити ваш обліковий запис. У розділі оберіть **“ПАРАМЕТРИ Й КОНФІДЕНЦІЙНІСТЬ”** (може також називатися **“КОНФІДЕНЦІЙНІСТЬ І БЕЗПЕКА”**) > перейдіть **“КОНФІДЕНЦІЙНІСТЬ”** > **“ВИДИМІСТЬ”** > потрібно вимкнути **“ПРОПОНУЙТЕ СВОЇ ОБЛІКОВІ ЗАПИСИ ІНШИМ”** (може також називатися **“РЕКОМЕНДУВАТИ МІЙ АКАУНТ”***)* > знайдіть свої **“КОНТАКТИ”** > відфільтруйте **“ХТО МОЖЕ НАДСИЛАТИ ВАМ ПРЯМІ**

ПОВІДОМЛЕННЯ”;

не дозволяйте іншим завантажувати свої відеоматеріали. Для цього у розділі оберіть **“ПАРАМЕТРИ Й КОНФІДЕНЦІЙНІСТЬ”** (може також називатися **“КОНФІДЕНЦІЙНІСТЬ І БЕЗПЕКА”**) > перейдіть **“КОНФІДЕНЦІЙНІСТЬ”** > **“ВЗАЄМОДІЇ”** свого облікового запису > перейдіть **“ЗАВАНТАЖИТИ”** > вимкнути **“ДОЗВОЛИТИ ІНШИМ ЗАВАНТАЖУВАТИ МОЇ ВІДЕО”**. Це запобігає збереженню ваших відеоматеріалів в іншому місці без вашого дозволу;

використовуйте VPN-технології високого рівня надійності. TikTok може легко отримати доступ до вашого місцезнаходження, використовуючи вашу IP-адресу або GPS, тому використання VPN-технології забезпечить вам більшу безпеку в Інтернеті.

ПАМ’ЯТАЙТЕ! В умовах війни категорично **ЗАБОРОНЕНО** фотографувати, знімати на відео та розміщувати і поширювати в Інтернеті:

місця дислокації, позиції, переміщення (маневр) військових частин (підрозділів) складових сил безпеки і оборони України;

блокпости, військові частини (підрозділи) та інші військово-промислові об’єкти;

результати вогневого ураження противника (так противник дізнається, куди влучив, оцінює масштаби ураження та коригує вогонь).

У додатках 2, 3, 4 до цих Методичних рекомендацій наведено порівняння безпеки користування месенджерами, які були отримані за результатами незалежних тестувань.

6. НАЛАШТУВАННЯ БЕЗПЕКИ СПІЛКУВАННЯ У СОЦІАЛЬНИХ МЕРЕЖАХ

За роки збройної агресії рф проти України в Інтернеті було зібрано велику кількість інформації, а саме: документів російських військовослужбовців, доказів щодо їхньої причетності до воєнних злочинів, даних про маршрути та місця пересування бойовиків і навіть особистих повідомлень. Соціальні мережі стали основним джерелом розвідки, тому необхідно розуміти, як від неї захиститися.

6.1. Налаштування доступу до своєї сторінки

Перше, на що дивляться спецслужби, – це профіль людини в соціальних мережах. Аватарка (фотографія користувача), дата народження, рід занять, зареєстровані групи тощо можуть розповісти про те, який спосіб життя веде людина і чим вона займається.

Уникнути статусу “клієнта” спецслужби дуже легко, адже достатньо лише не надавати реальної інформації про себе або надавати її частково. Для цього зробіть певні налаштування в розділі **“НАЛАШТУВАННЯ ПРИВАТНОСТІ”**, а саме:

закрийте доступ до персональної інформації (дата народження, номер телефону тощо) всім користувачам, окрім друзів. Дуже важливо закрити також доступ для друзів друзів;

у всіх соціальних мережах розділіть друзів по групах. Створіть спеціальну групу для “ненадійних друзів” (яких ви не знаєте у реальному житті) та обмежте їхні права на рівні звичайних користувачів;

закрийте можливість перегляду фото та відеоматеріалів усім користувачам, крім друзів;

не надавайте інформації про місце роботи/служби, рік закінчення школи, вишу тощо. Якщо написали раніше, то обов’язково видаліть.

Налаштувавши таким чином доступ до своєї сторінки, всі, окрім друзів, бачитимуть лише ваше ім’я, фото та інформацію, якою ви поділилися на своїй сторінці.

6.2. Заходи безпеки при завантаженні фото на свою сторінку

Основним джерелом інформації із соціальних мереж є фотографії. При завантаженні фотографій слід дотримуватися таких запобіжних заходів:

по-перше, необхідно вимкнути геотегування або геопозиціонування. На багатьох девайсах за умовчанням до фотографії додається службова інформація, яка вказує на місце і час зйомки;

по-друге, перш ніж надсилати свіжі фотографії, подумайте про фон. Навіть одне дерево або дорожній знак можуть стати так званою характерною особливістю місцевості, що дозволить експертам точно визначити, де саме було зроблено фото. Викладаючи фото, обов’язково зафарбовуйте обличчя, окремі об’єкти (або навіть весь фон), маркування озброєння, військової техніки чи будь-що інше, що може ідентифікувати місце, де було зроблено фото;

по-третє, не поспішайте викладати фотографії. Навіть якщо фотографія безпечна і не дає ворогові жодної корисної інформації, якусь незначну деталь можна не помітити. Не публікуйте фото одразу після того, як вони були зроблені, а зачекайте, поки вони втратять актуальність. Найкраще це робити через два-три місяці, коли відбудеться ротація військ або зміниться пора року і зникнуть характерні риси місцевості.

7. НАЛАШТУВАННЯ БЕЗПЕКИ В БРАУЗЕРІ

7.1. Google Chrome

У меню браузера перейдіть до налаштувань та оберіть пункт **“КОНФІДЕНЦІЙНІСТЬ І БЕЗПЕКА”** і виконайте такі маніпуляції:

налаштування безпеки > рекомендується залишити обраний пункт **“СТАНДАРТНИЙ ЗАХИСТ”**, **“ПОСИЛЕНИЙ ЗАХИСТ”** передбачає підвищення безпеки під час перегляду вебсторінок, але тим самим він збільшує обсяг даних, які ваш браузер надсилає на сервери компанії Google. В підменю **“РОЗШИРЕНІ”** перевірте наявність встановленої опції **“ЗАВЖДИ**

ВИКОРИСТОВУВАТИ НАДІЙНІ З'ЄДНАННЯ";

налаштування файлів cookie > оберіть **"КОНФІДЕНЦІЙНІСТЬ ТА БЕЗПЕКА"** > **"ФАЙЛИ СООКІЕ ТА ІНШІ ДАНІ ІЗ САЙТІВ"** > виберіть такі опції:

"БЛОКУВАТИ СТОРОННІ ФАЙЛИ СООКІЕ";

"ВИДАЛЯТИ ФАЙЛИ СООКІЕ Й ДАНІ САЙТІВ, КОЛИ ЗАКРИВАЮТЬСЯ ВСІ ВІКНА";

"НАДСИЛАТИ ЗАПИТ "НЕ ВІДСТЕЖУВАТИ" РАЗОМ ІЗ ТРАФІКОМ ВЕБПЕРЕГЛЯДУ", щоб зменшити відстеження переміщень користувача між сайтами;

вимкніть спливаючі повідомлення > оберіть **"КОНФІДЕНЦІЙНІСТЬ ТА БЕЗПЕКА"** > **"НАЛАШТУВАННЯ САЙТІВ"** > **"ПОВІДОМЛЕННЯ"** > деякі сайти вимагають дозволу на надсилання сповіщень, вимкніть цю опцію > **"ДОЗВОЛИТИ"** > перегляньте сайти з дозволом на відправлення і вимкніть усі ті, які вас не цікавлять або непотрібні;

вимкнення спливаючих вікон в Google Chrome > оберіть **"КОНФІДЕНЦІЙНІСТЬ ТА БЕЗПЕКА"** > **"НАЛАШТУВАННЯ САЙТІВ"** > **"КОНТЕНТ"** > **"СПЛИВАЮЧІ ВІКНА/ПЕРЕСПРЯМУВАННЯ"** > встановіть **"ЗАБЛОКОВАНО"**;

видалення вірусів у Google Chrome та шкідливих розширень у браузері > оберіть **"КОНФІДЕНЦІЙНІСТЬ ТА БЕЗПЕКА"** > **"ПЕРЕВІРКА СИСТЕМИ"** > оберіть **"ПЕРЕВІРИТИ"**;

оновлення браузера.

Якщо висвітилося у правому верхньому куті браузера повідомлення, що є нова версія, встановіть її. Кожна нова версія є швидкою та безпечнішою.

7.2. Microsoft Edge

У меню браузера перейдіть до налаштувань та оберіть пункт **"КОНФІДЕНЦІЙНІСТЬ, ПОШУК І СЛУЖБИ"** і виконайте такі маніпуляції:

налаштування запобігання відстеженню > рекомендується залишити обраний пункт **"ЗБАЛАНСОВАНА"**, **"СУВОРО"** – до всіх сайтів застосовується додатковий захист безпеки. Суворий режим може вплинути на можливість виконання звичайних завдань в Інтернеті, оскільки деякі частини вебсайтів можуть працювати не правильно;

налаштування видалення даних про перегляд вебсторінок > оберіть **"ВИБІР ЕЛЕМЕНТІВ, ЯКІ ПОТРІБНО ВИДАЛЯТИ ПІД ЧАС КОЖНОГО ЗАКРИТТЯ БРАУЗЕРА"** > виберіть такі опції:

"Журнал браузера";

"Журнал завантажень";

"Файли cookie та інші дані сайтів";

"Кешовані зображення та файли";

"Паролі";

"Дані для автозаповнення форм (включно з формами та картками)";

“Дозволи для сайтів”;

налаштування конфіденційності > виберіть такі опції:

увімкніть **“НАДСИЛАТИ ЗАПИТ “НЕ ВІДСТЕЖУВАТИ”**;

вимкніть **“ДОЗВОЛИТИ САЙТАМ ПЕРЕВІРЯТИ, ЧИ Є У ВАС ЗБЕРЕЖЕНІ МЕТОДИ ОПЛАТИ”**;

налаштування безпеки > виберіть такі опції:

“ФІЛЬТР SMARTSCREEN ДЛЯ MICROSOFT DEFENDER”;

“БЛОКУВАННЯ ПОТЕНЦІЙНО НЕБАЖАНИХ ПРОГРАМ”;

“ЗАХИСТ ВЕБСАЙТУ ВІД ДРУКАРСЬКИХ ПОМИЛОК”;

“УВІМКНІТЬ СЛУЖБИ БЕЗПЕКИ САЙТІВ, ЩОБ ОТРИМАТИ ДОДАТКОВІ ВІДОМОСТІ ПРО САЙТИ, ЯКІ ВИ ВІДВІДУЄТЕ”;

“ВИКОРИСТОВУЙТЕ БЕЗПЕЧНИЙ DNS, ЩОБ УКАЗАТИ СПОСІБ ПОШУКУ МЕРЕЖЕВОЇ АДРЕСИ ВЕБСАЙТІВ”.

Своєчасно оновлюйте браузер. Для цього перейдіть **“ПАРАМЕТРИ”** > **“ПРО MICROSOFT EDGE”** > **“ПРО ПРОГРАМУ”** > щоб завершити оновлення, перезапустіть Microsoft Edge **“ПЕРЕЗАВАНТАЖИТИ”**. Якщо оновлення відсутні, буде зазначено, що використовується актуальна версія Microsoft Edge.

У додатках 5, 6, 7 до цих Методичних рекомендацій наведено порівняння веббраузерів за визначеними критеріями.

8. ОСНОВИ БЕЗПЕЧНОЇ РОБОТИ З ЕЛЕКТРОННОЮ ПОШТОЮ

Для безпечної роботи з електронною поштою необхідно дотримуватися певних кроків:

1. Використання захищеного з’єднання.

Завжди використовуйте захищений поштовий протокол, особливо якщо користуєтеся бездротовою мережею. Налаштуйте свій поштовий клієнт на використання параметра безпеки (TLS – захищений транспортний протокол безпеки), протоколи (Secure IMAP or Secure POP3 – інтернет-протоколи для роботи з поштовими повідомленнями) для шифрування ваших листів під час їх передачі між сервером та користувачем.

2. Використання надійного паролю під час реєстрації пошти.

Безпека акаунта починається вже під час реєстрації електронної пошти. Надійний пароль має бути випадковим та унікальним (або таким, що складно відтворити) набором букв, цифр та спеціальних символів. Крім того, чим довший пароль, тим він надійніший!

Не використовуйте один пароль для різних акаунтів та функцію автозбереження паролів на пристрої.

3. Здійснення прив’язки номера свого телефону до акаунта.

Для додаткового захисту електронної пошти від спроб зламу, підвищення безпеки акаунта та можливості швидкого відновлення доступу до пошти власником поштового сервісу впроваджено систему, яка використовує девайси для автентифікації та верифікації користувачів на етапі реєстрації електронної пошти. За цих умов система генерує унікальний код під час створення

облікового запису та надсилає його на номер телефону, вказаний під час реєстрації електронної пошти. Це забезпечує більш безпечну та надійну роботу з електронною поштою.

4. Уникнення підозрілих посилань у пошті.

Серед способів захисту електронної пошти від зламу варто згадати про “фішинг” – отримання доступу до конфіденційних даних користувачів, а саме логіна та пароля. Це один з найпоширеніших способів зламу електронної пошти, але насправді від нього дуже легко захиститися.

Звертайте увагу на зміст листа одержувача, уважно подивіться на електронну адресу листа, з якої він надійшов на вашу електронну пошту. Утримайтеся від відкриття прикріплених файлів чи посилань у невідомих листах. Дотримуйтеся кібергігієни, не відкривайте невідомі листи, не переходьте за посиланнями та не завантажуйте додатки до листа. Перевірте легітимність листа іншим методом (за можливості спитайте особисто автора) та видаліть лист, якщо інформація не підтвердилася.

Ніколи не відкривайте листи з дивовижними пропозиціями чи сповіщеннями (наприклад, про отримання винагороди, особливо якщо участі у розіграші не брали), які надто привабливі, щоб бути правдою.

5. Дії у разі зламу акаунта.

Якщо вас зламали, необхідно виконати такі дії:

перевірте девайс (комп’ютер) ліцензійним антивірусним програмним забезпеченням, немає сенсу змінювати пароль до електронної пошти, доки девайс (комп’ютер) заражений вірусами;

зверніться до служби технічної підтримки, щоб відновити доступ до вашої електронної пошти, і зазначте, що вашу електронну пошту було зламано, ними буде обов’язково вжито додаткових заходів.

6. Дії для захисту акаунта від зламу.

Рекомендації:

видаліть або заблокуйте ті облікові записи, які наразі не використовуються;

періодично перевіряйте звіти в системах безпеки акаунтів сервісів, які ілюструють вашу активність та перелічують пристрої, з яких ви входили у ваш обліковий запис. Будь-які незнайомі пристрої можуть бути заблоковані;

вимкніть або заблокуйте сторонні сервіси. Ця порада особливо актуальна для соціальної мережі Facebook. Багато користувачів Інтернету і цієї соцмережі стикалися з ситуаціями, коли після використання сторонніх сервісів із входом через акаунт Facebook дані цих користувачів “випадково потрапляли в мережу”;

у тому ж Facebook ви можете вказати контакти, які будуть використані для відновлення доступу до вашого акаунта в разі потреби;

періодично змінюйте паролі у всіх акаунтах, у тому числі й імейл-акаунті;

якщо ви хочете підключитися до Інтернету в незнайомому мережевому середовищі, обов'язково використовуйте VPN-технологію. Для цього використовується окреме програмне забезпечення, доступне для завантаження з Google Play (для пристроїв під операційною системою Android) та App Store (для пристроїв під операційною системою iOS);

стежте за своїми публікаціями в соціальних мережах. Публікація фотографій або скриншотів екрана девайса (комп'ютера) може призвести до випадкового витоку інформації у "відкриту мережу".

9. ОСНОВНІ АСПЕКТИ БЕЗПЕЧНОЇ РОБОТИ ІЗ СИСТЕМАМИ ВІДЕОКОНФЕРЕНЦІЙ

З метою безпечної роботи із системами відеоконференцій користуйтеся певними правилами:

1. Підготуйте належне середовище для роботи.

Витік даних часто трапляється ненавмисно. Наприклад, конфіденційна інформація з попередньої онлайн-зустрічі може бути залишена на дошці для записів позаду. Тому перед початком розмови переконайтеся, що в полі зору вебкамери немає конфіденційних даних.

2. Налаштуйте контроль доступу.

Більшість платформ для проведення відеоконференцій дають можливість створювати групи користувачів або обмежувати доступ через Інтернет-домен, щоб лише певна кількість людей могла приєднатися до дзвінка.

Щоб підвищити безпеку відеоконференції, встановіть пароль. Як правило, пароль генерується автоматично під час створення конференції, і всі запрошені до конференції мають ввести пароль. Однак пароль не повинен бути прикріплений до посилання на конференцію. Ініціатор конференції також може повністю контролювати, хто підключається до розмови, залишаючи користувачів у режимі очікування.

3. Налаштуйте безпечну передачу файлів.

У багатьох додатках відеозв'язок шифрується за умовчанням. Деякі сервіси за умовчанням шифрують лише чати, і в цьому випадку доведеться самостійно налаштовувати шифрування відеозв'язку. Окремі додатки дають можливість встановлювати обмеження на типи файлів, які надсилають учасники. Наприклад, можна заборонити надсилання виконуваних файлів формату .exe.

Обираючи сервіс для організації відеозв'язку, рекомендовано користуватися тим, що забезпечує наскрізне шифрування.

3.1. Для прикладу, Zoom (одна з найпоширеніших програм для організації відеоконференцій) не здійснює наскрізного шифрування відеозв'язку. Для шифрування необхідно зайти на Zoom Web Portal та перейти до**"НАЛАШТУВАННЯ"** > **"КОНФЕРЕНЦІЯ"** > **"БЕЗПЕКА"** та перевірити функцію **"ДОЗВОЛИТИ НАСКРІЗНЕ ШИФРУВАННЯ"**. Для її активації необхідно натиснути перемикач. Після появи діалогового вікна підтвердження необхідно обрати **"УВІМКНУТИ"** для підтвердження змін. У розділі

“БЕЗПЕКА” обрати **“ТИП ШИФРУВАННЯ ЗА УМОВЧЕННЯМ”** та зберегти зміни.

3.2. В іншому сервісі для онлайн зустрічей – Google Meet (раніше Duo) – наскрізне шифрування є стандартним методом захисту даних під час комунікації. Коли ви телефонуєте безпосередньо користувачу (під час дзвінків з одним абонентом або групою), використовується наскрізне шифрування, що маскує дані за допомогою коду, до якого маєте доступ лише ви й ваші співрозмовники. Під час такого виклику відображатимуться значок замка і водяний знак, які підтверджуватимуть, що використовується наскрізне шифрування. Але слід зауважити, що у Google Meet, крім відеодзвінків, також реалізовано функцію зустрічей, у яких замість наскрізного застосовується хмарне шифрування, що захищає дані під час пересилання та зберігання в центрах обробки даних Google.

4. Управління залученням учасників.

Більшість платформ дають можливість контролювати, хто і коли приєднався до дзвінка. Це можна відстежити або за тим, хто із зареєстрованих учасників приєднався, або за списком учасників, який можливо завантажити після завершення дзвінка. Список учасників часто містить інформацію про те, коли користувачі приєдналися і коли вони від’єдналися, тому можна побачити, чи був певний користувач присутнім протягом усього часу дзвінка.

5. Встановіть обмеження доступу до екрана.

Обмежте можливість спільного доступу до екрана для хоста або людини, яка обирає хост. Таким чином можна уникнути ризику витоку даних. Надаючи спільний доступ до екранів, діліться лише потрібними програмами, а не всім робочим столом. Це пов’язано з тим, що піктограми та назви файлів на робочому столі також можуть містити конфіденційну інформацію.

10. ОСНОВИ БЕЗПЕЧНОГО КОРИСТУВАННЯ БЕЗПРОВОДОВИМИ МЕРЕЖАМИ (Wi-Fi)

З метою безпечної роботи з безпроводовими мережами (Wi-Fi) дотримуйтеся певних правил:

1. Захист пристроїв маршрутизації.

Ваш інтернет-провайдер може надавати власний модем/роутер для вас, це буде частиною договору. Щоб максимально отримати адміністративний контроль над функціями маршрутизації та бездротового зв’язку вашої домашньої мережі, розгляньте можливість використання особистого пристрою маршрутизації, який підключається до модема/маршрутизатора, наданого провайдером. Крім того, використовуйте сучасні функції маршрутизатора, щоб створити окрему бездротову мережу для гостей та відокремити мережу від довірених та приватних пристроїв.

Маршрутизатор є шлюзом до вашої домашньої мережі. Без належної безпеки та виправлень він, швидше за все, буде скомпрометований, що призведе до компрометації інших пристроїв у мережі. Щоб мінімізувати вразливі місця та підвищити безпеку, потрібно оновлювати операційну систему

маршрутизатора до останньої версії, бажано налаштувати автоматичне оновлення. У разі, якщо виробник закінчив підтримку зазначеного обладнання, бажано його замінити. Це забезпечить стабільне оновлення та усунення вразливостей після їх виявлення.

2. Використання протоколу захисту WPA3 та/або WPA2.

Для збереження конфіденційності бездротового зв'язку переконайтеся, що ваш особистий або наданий провайдером маршрутизатор підтримує Protected Access 3 (WPA3). Якщо у вашій мережі є пристрої, які не підтримують WPA3, ви можете обрати WPA2/3. Таке рішення дасть можливість новим пристроям використовувати більш захищений протокол, але й залишить можливість підключення старіших пристроїв до мережі з використанням WPA2.

Коли налаштовуєте WPA3 чи WPA2/3, використовуйте надійний пароль. Пам'ятайте, чим складніший пароль, тим менша можливість його компрометації. Якщо доступно, для більшої надійності активуйте захист адміністративного доступу. Більшість девайсів сьогодні підтримують WPA3 та/або WPA2. Якщо ви плануєте придбати новий пристрій, переконайтеся, що він сертифікований WPA3-Personal. Змініть стандартний ідентифікатор мережі (SSID) на унікальний. Не приховуйте SSID, тому що це не захистить вашу мережу, але може призвести до проблем сумісності з використовуваними пристроями.

3. Налаштуйте адміністрування тільки з внутрішньої мережі.

Вимкніть можливість віддаленого доступу до адміністрування маршрутизатора. Для більшої безпеки можливість внесення змін до конфігурації самої мережі повинна надаватися лише пристроям з внутрішньої мережі, для цього необхідно вимкнути в налаштуваннях маршрутизатору Universal Plug-n-Play (UPnP). Ці заходи допоможуть закрити вразливості, використавши які зловмисник може скомпрометувати вашу мережу.

4. Використання публічних точок доступу.

В основному громадські місця, такі як кафе, готелі чи аеропорти тощо, пропонують бездротові точки доступу чи місця, де користувач може отримати безкоштовний доступ до Інтернету. Оскільки базова інфраструктура цих мереж невідома, а безпека може бути слабкою, такі точки доступу часто є ціллю для зловмисників, тому потрібно уникати прямого підключення до громадських бездротових мереж. За можливості використовуйте корпоративну чи персональну точку доступу з надійною автентифікацією та шифруванням. Якщо необхідно використати публічну точку доступу, дотримуйтеся таких рекомендацій:

використовуйте стільникову мережу для доступу в Інтернет замість публічних точок доступу. Функція захисту забезпечується провайдером стільникового зв'язку;

використовуйте надійну VPN-технологію під час підключення до публічного Wi-Fi. Це допоможе захистити ваше з'єднання від зловмисних дій;

забезпечуйте захист від фізичного доступу сторонніх осіб. Не залишайте девайси без нагляду в публічних місцях.

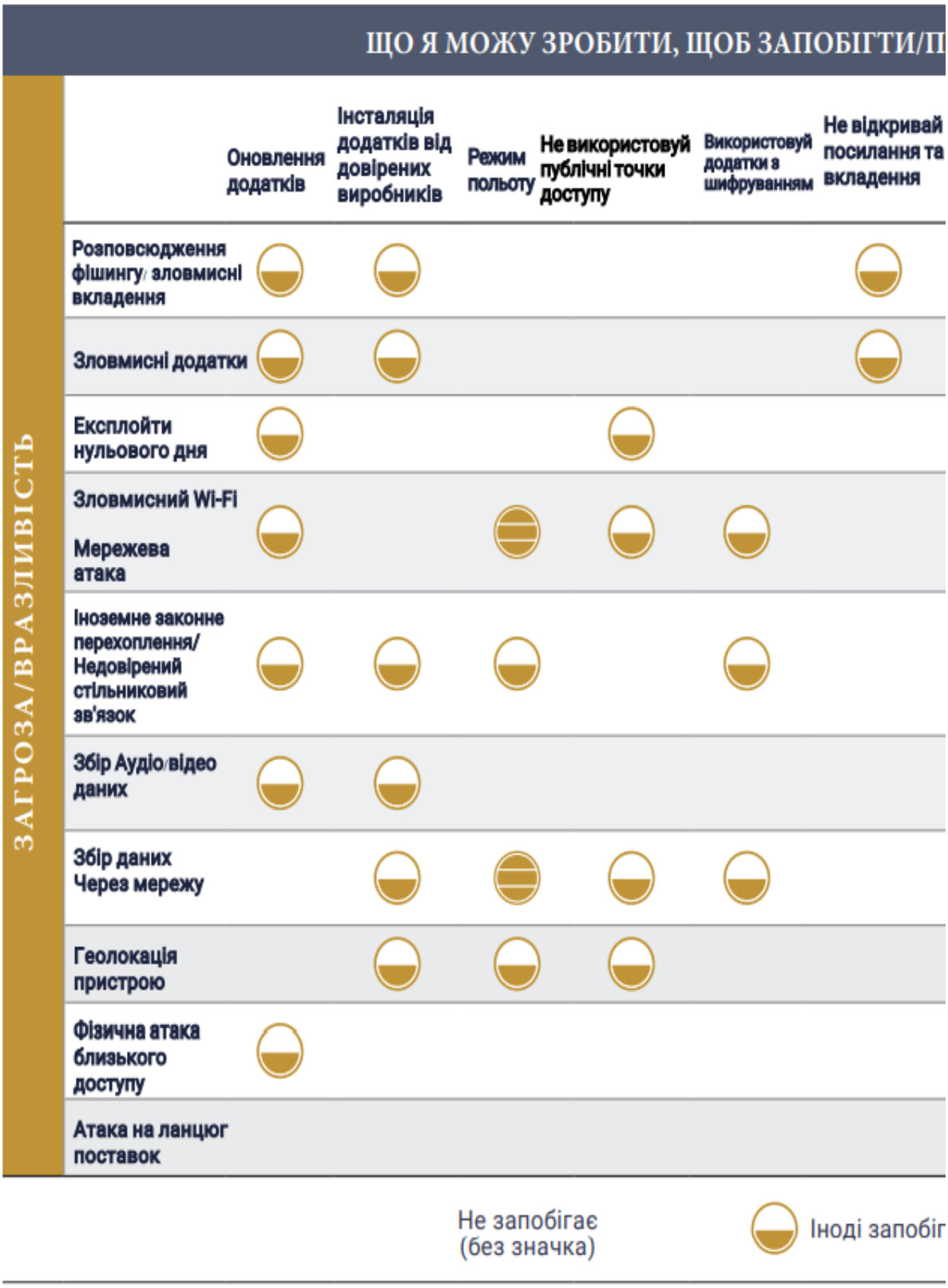
Заступник командувача Військ зв'язку
та кібербезпеки Збройних Сил України
полковник Віктор ЛІСАКОНОВ

Додаток 1
до Методичних рекомендацій з питань забезпечення особистої кібербезпеки військовослужбовця (розділ 4)

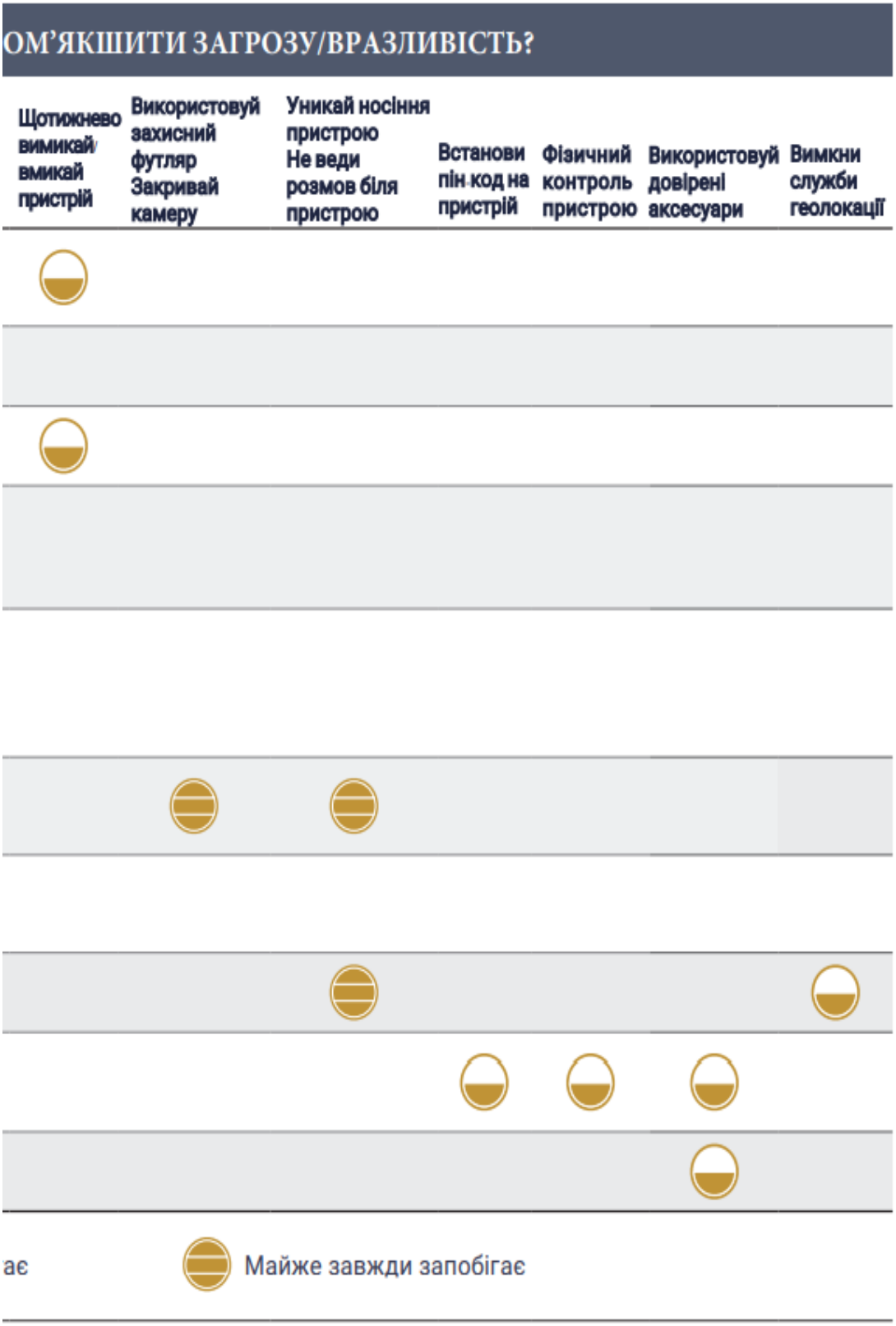
Найкращі практики налаштувань мобільних пристроїв

Продовження додатка 1

Продовження додатка 1



Продовження додатка 1



Додаток 2
до Методичних рекомендацій з питань забезпечення особистої кібербезпеки військовослужбовця (розділ 5)

Порівняння безпеки користування месенджерами Google Messages, Apple iMessage, Facebook Messenger, Element/Riot

Критерії оцінки	Назва месенджера			
	Google Messages	**Apple iMessage**	**Facebook Messenger**	**Element / Riot**
Чи рекомендується програма для захисту моїх повідомлень і вкладень?	Ні	Ні	Ні	Ні
Основні причини, чому програма не рекомендована **Покращення рекомендованих програм**	Названо партнером АНБ у викриттях Сноудена Заробляє гроші на особистих даних Дані незахищені, не всі дані захищені Немає незалежного та останнього аудиту коду та аналізу безпеки Закритий код	Названо партнером АНБ у викриттях Сноудена Дані незахищені, не всі дані захищені Немає незалежного та останнього аудиту коду та аналізу безпеки Закритий код	Названо партнером АНБ у викриттях Сноудена Шифрування не ввімкнено за умовчанням Заробляє гроші на особистих даних Дані незахищені, не всі дані захищені Немає незалежного та останнього аудиту коду та аналізу безпеки Закритий код	Немає незалежного та останнього аудиту коду та аналізу безпеки
Юрисдикція компанії	США	США	США	Великобританія
Інфраструктурна юрисдикція	У всьому світі (розповсюдження триває, невідомі точні місця, швидше за все, регіони Google Cloud)	США (заплановані Ірландія та Данія); iMessage працює на AWS і Google Cloud	США, Швеція (планується Ірландія)	Великобританія (і потенційно всі юрисдикції, оскільки це децентралізована платформа обміну повідомленнями)

Продовження додатка 2

Критерії оцінки	Назва месенджера			
	Google Messages	**Apple iMessage**	**Facebook Messenger**	**Element / Riot**
Причетний до передачі даних клієнтів спецслужбам?	Так	Так	Так	Ні
Можливість спостереження вбудована в додаток?	Ні	Ні	Ні	Ні
Чи надає компанія звіт про прозорість?	Так	Так	Так	Ні
Загальна позиція компанії щодо конфіденційності клієнтів	Не підтримує	Не підтримує	Не підтримує	Підтримує
Фінансування	Google	Apple	Facebook	New Vector Limited
Компанія збирає дані клієнтів?	Так	Так	Так	Ні
Додаток збирає дані клієнтів?	Так (Важко оцінити, оскільки додаток інтегровано в ширшу екосистему Google)	Так (Важко оцінити, оскільки програма інтегрована в ширшу екосистему Apple)	Здоров'я та фітнес / покупки / фінансова інформація / місцезнаходження / контактна інформація / контакти / вміст користувача / історія пошуку / історія вебперегляду / ідентифікатори / дані про використання / конфіденційна інформація / діагностика / інші дані	Контактна інформація / контакти / ідентифікатори / діагностика / вміст користувача (Контактна інформація не надсилається при анонімному використанні)
Дані користувача та/або метадані, надіслані материнській компанії та/або третім особам?	Так	Так	Так	Ні (у разі здійснення платежу дані користувача надсилаються третій стороні)

Продовження додатка 2

Критерії оцінки	Назва месенджера			
	Google Messages	**Apple iMessage**	**Facebook Messenger**	**Element / Riot**
Шифрування ввімкнено за умовчанням?	Так	Так	Ні	Так
Криптографічні примітиви	Curve25519 / AES-256 / HMAC-SHA256	RSA-1280 (шифрування), ECDSA 256 (підпис) / AES 128 / SHA-1	Curve25519 / AES-256 / HMAC-SHA256	Curve25519 / AES-256 / HMAC-SHA256
Чи програма та сервер повністю відкриті?	Ні	Ні	Ні	Так (клієнти Element / Riot, сервер/API matrix.org)
Чи використовуються відтворювані збірки для перевірки додатків на вихідний код?	Ні	Ні	Ні	Ні
Чи можете ви зареєструватися в програмі анонімно?	Ні	Ні	Ні	Так
Чи можете ви додати контакт, не довіряючи серверу каталогів?	Google Повідомлення використовує RCS, який не використовує службу каталогів	Ні	Ні	Ні
Чи можете ви вручну перевірити відбитки пальців контактів?	Так	Ні	Так	Так
Службу каталогів можна змінити, щоб увімкнути атаку MITM?	Google Повідомлення використовує RCS, який не використовує службу каталогів	Так	Так	Так
Чи отримуєте ви сповіщення про зміну відбитка пальця контакту?		Ні		Так

Продовження додатка 2

Критерії оцінки	Назва месенджера			
	Google Messages	**Apple iMessage**	**Facebook Messenger**	**Element / Riot**
Чи хешується особиста інформація (номер мобільного телефону, список контактів тощо)?	Google Повідомлення використовує RCS, який не використовує службу каталогів	Ні	Ні	Так
Чи створює та зберігає програма закритий ключ на самому пристрої?	Так	Так	Так	Так
Чи може компанія читати повідомлення?	Ні	Ні	Так	Ні
Чи підтримує додаток повну секретність?	Так	Ні	Так	Так
Чи шифрує програма метадані?	Ні	Ні	Ні	
Чи використовує програма TLS/Noise для шифрування мережевого трафіку?	Так	Так	Так	Так
Чи використовує програма закріплення сертифіката?		Так (>=iOS 9.3)		
Чи шифрує програма дані на пристрої? (тільки для iOS і Android)	Ні	Так (якщо ввімкнено парольну фразу)		Так
Чи допускає програма вторинний фактор автентифікації?	Ні	Ні	Ні	Ні
Чи зашифровані повідомлення під час резервного копіювання в хмару?	Так (>= Android P)	Ні		Так
Чи реєструє компанія мітки часу/IP-адреси?		Так	Так	

Продовження додатка 2

Критерії оцінки	Назва месенджера			
	Google Messages	**Apple iMessage**	**Facebook Messenger**	**Element / Riot**
Чи проводився нещодавно аудит коду та незалежний аналіз безпеки?	Ні	Ні	Ні	Ні (бібліотека шифрування Matrix перевірена незалежною стороною)
Чи задокументовано проект?	Ні	Частково	Частково	Частково
Чи є в програмі повідомлення, що самознищуються?	Немає	Немає	Так	Немає

Додаток 3
до Методичних рекомендацій з питань забезпечення особистої кібербезпеки військовослужбовця (розділ 5)

Порівняння безпеки користування месенджерами Signal, Microsoft Skype, Telegram, Threema, Viber

Критерії оцінки	Назва месенджера				
	Signal	**Microsoft Skype**	**Telegram**	**Threema**	**Viber**
Чи рекомендується програма для захисту моїх повідомлень і вкладень?	Так	Ні	Ні	Так	Ні
Основні причини, чому програма не рекомендована **Покращення рекомендованих програм**	Скасувати обов'язкову вимогу для користувачів реєструватися за допомогою номера мобільного телефону Надати більш повну незалежну оцінку безпеки/конфіденційності	Названо партнером АНБ у викриттях Сноудена Шифрування не ввімкнено за умовчанням Заробляє гроші на особистих даних Дані незахищені, не всі дані захищені Закрите джерело	Спеціальна криптографія Шифрування не ввімкнено за умовчанням Дані незахищені, не всі дані захищені	Зробіть API та код сервера відкритими Забезпечте більш повну незалежну оцінку безпеки/конфіденційності	Дані незахищені, не всі дані захищені Немає незалежного та останнього аудиту коду та аналізу безпеки Закритий код
Юрисдикція компанії	США	США	США / Великобританія / Беліз / ОАЕ	Швейцарія	Люксембург / Японія
Інфраструктурна юрисдикція	США	США, Нідерланди, Австралія, Бразилія, Китай, Ірландія, Гонконг і Японія	Великобританія, Сінгапур, США та Фінляндія	Швейцарія	США

Продовження додатка 3

Критерії оцінки	Назва месенджера				
	Signal	**Microsoft Skype**	**Telegram**	**Threema**	**Viber**
Причетний до передачі даних клієнтів спецслужбам?	Ні	Так	Ні	Ні	Ні
Можливість спостереження вбудована в додаток?	Ні	Так	Ні	Ні	Ні
Чи надає компанія звіт про прозорість?	Так	Так	Ні	Так	Ні
Загальна позиція компанії щодо конфіденційності клієнтів	Підтримує	Не підтримує	Не підтримує	Підтримує	Не підтримує
Фінансування	Freedom of the Press Foundation / the Knight Foundation / the Shuttleworth Foundation / the Open Technology Fund / Signal Foundation (Brian Acton)	Microsoft	Павло Дуров	Користувач платить / Afinum Management AG	Rakuten / друзі та родина Талмона Марко (дуже незрозуміло)
Компанія збирає дані клієнтів?	Ні	Так	Так	Ні	Так
Додаток збирає дані клієнтів?	Контактна інформація	Так (інформація не надіслана в Apple Store)	Контактна інформація / контакти / ідентифікатори	Контактна інформація/ідентифікатори/діагностика (контактна інформація не надсилається при анонімному використанні)	Місцезнаходження / ідентифікатори / покупки / місцезнаходження / контактна інформація / контакти / ідентифікатори / дані про використання / вміст користувача / дані про використання / діагностика

Продовження додатка 3

Критерії оцінки	Назва месенджера				
	Signal	**Microsoft Skype**	**Telegram**	**Threema**	**Viber**
Дані користувача та/або метадані, надіслані материнській компанії та/або третім особам?	Мінімальний (обов'язковий номер мобільного телефону, надісланий третій стороні для реєстрації та відновлення)	Так	Так	Ні (додатковий номер мобільного телефону, надісланий третій стороні для реєстрації)	Так
Шифрування ввімкнено за умовчанням?	Так	НІ	Ні	Так	Так (якщо пристрій це підтримує)
Криптографічні примітиви	Curve25519 / AES-256 / HMAC-SHA256	RSA-1536 і 2048 / AES 256 / SHA-1	RSA 2048 / AES 256 / SHA-256	Curve25519 256 / XSalsa20 256 / Poly1305-AES 128	Curve25519 256 / Salsa20 128 / HMAC-SHA256
Чи програма та сервер повністю відкриті?	Так	Ні	Ні (лише клієнти та API)	Ні (лише програми)	Ні
Чи використовуються відтворювані збірки для перевірки додатків на вихідний код?	Тільки Android	Ні	iOS і Android	Тільки Android	Ні
Чи можете ви зареєструватися в програмі анонімно?	Ні	Ні	Ні	Так	Ні
Чи можете ви додати контакт, не довіряючи серверу каталогів?	Ні	Ні	Ні	Так	Так

Продовження додатка 3

Критерії оцінки	Назва месенджера				
	Signal	**Microsoft Skype**	**Telegram**	**Threema**	**Viber**
Чи можете ви вручну перевірити відбитки пальців контактів?	Так	Ні	Ні (лише сеанс, не надає інформацію про відбитки пальців користувачів)	Так	Так
Службу каталогів можна змінити, щоб увімкнути атаку MITM?	Так	Так	Так	Так	Так
Чи отримуєте ви сповіщення про зміну відбитка пальця контакту?	Так	Ні	Ні (лише сеанс, не надає інформації про відбитки пальців користувачів)	Так	Так
Чи хешується особиста інформація (номер мобільного телефону, список контактів тощо)?	Переважно	Ні	Ні	Так	Ні
Чи програма створює та зберігає закритий ключ на самому пристрої?	Так		Так	Так	Так
Чи може компанія читати повідомлення?	Ні	Так	Так	Ні	Ні
Чи підтримує додаток повну секретність?	Так		Ні (сеансові ключі змінюються після 100 разів використання)	Так	Так

Продовження додатка 3

Критерії оцінки	Назва месенджера				
	Signal	**Microsoft Skype**	**Telegram**	**Threema**	**Viber**
Чи шифрує програма метадані?	Так		Ні	Так	
Чи використовує програма TLS/Noise для шифрування мережевого трафіку?	Так	Так	Ні	Так	Так
Чи використовує програма закріплення сертифіката?	Так			Так	
Чи шифрує програма дані на пристрої? (тільки для iOS і Android)	Так (якщо ввімкнено парольну фразу)			iOS: так (якщо ввімкнено парольну фразу); Android: так (якщо головний ключ установлено в додатку)	
Чи допускає програма вторинний фактор автентифікації?	Так	Ні	Так	Так	Ні
Чи зашифровані повідомлення під час резервного копіювання в хмару?	Signal виключено з резервних копій iCloud/iTunes і Android			Так	
Чи реєструє компанія мітки часу/IP-адреси?	Ні	Так	Так	Ні	Так
Чи проводився нещодавно аудит коду та незалежний аналіз безпеки?	Так (жовтень, 2014)	Немає	Так (листопад, 2015)	Так (жовтень, 2020)	Ні

Продовження додатка 3

Критерії оцінки	Назва месенджера				
	Signal	**Microsoft Skype**	**Telegram**	**Threema**	**Viber**
Чи добре задокументовано проект?	Частково	Ні	Частково	Частково	Частково
Чи є в програмі повідомлення, що самознищуються?	Так	Ні	Так	Ні	Так

Додаток 4
до Методичних рекомендацій з питань забезпечення особистої кібербезпеки військовослужбовця (розділ 5)

Порівняння безпеки користування месенджерами Facebook WhatsApp, Amazon Wickr Me, Wire, Session

Критерії оцінки	Назва месенджера			
	Facebook WhatsApp	**Amazon Wickr Me**	**Wire**	**Session**
Чи рекомендується програма для захисту моїх повідомлень і вкладень?	Ні	Ні	Так	Так
Основні причини, чому програма не рекомендована **Покращення рекомендованих програм**	Названо партнером АНБ у викриттях Сноудена Повідомлення можуть бути прочитані Facebook, якщо вони позначені як “образливі” Заробляє гроші на особистих даних Дані незахищені, не всі дані захищені Немає незалежного та останнього аудиту коду та аналізу безпеки Закритий код	Колишній керівник АНБ Кіт Александер входить до ради директорів Amazon. Фінансується ЦРУ Останні перевірки безпеки не є публічними Закрите джерело	Додатково обмежте зберігання та журналювання метаданих Забезпечте більш комплексну незалежну оцінку безпеки/конфіденційності	Запровадження ідеальної прямої секретності на рівні наскрізного шифрування Забезпечення більш комплексної незалежної оцінки безпеки/конфіденційності
Юрисдикція компанії	США	США	США / Швейцарія	Австралія

Продовження додатка 4

Критерії оцінки	Назва месенджера			
	Facebook WhatsApp	**Amazon Wickr Me**	**Wire**	**Session**
Інфраструктурна юрисдикція	США (інші місця невідомі)	США (інші місця невідомі)	ЄС	За повідомленням, у всьому світі (використовує децентралізовані сервери) За вкладенням, централізований сервер у Канаді
Причетний до передачі даних клієнтів спецслужбам?	Так	Ні	Ні	Ні
Можливість спостереження вбудована в додаток?	Ні	Ні	Ні	Ні
Чи надає компанія звіт про прозорість?	Так	Так	Так	Так
Загальна позиція компанії щодо конфіденційності клієнтів	Не підтримує	Не підтримує	Підтримує	Підтримує
Фінансування	Facebook	Amazon / ЦРУ	Janus Friis / Iconical / Zeta Holdings Luxembourg / Morpheus Ventures	LAG Foundation Ltd
Компанія збирає дані клієнтів?	Так	Так	Ні	Ні
Чи є в програмі повідомлення, що самознищуються?	Так	Так	Так	Так

Продовження додатка 4

Критерії оцінки	Назва месенджера			
	Facebook Whatsapp	**Amazon Wickr Me**	**Wire**	**Session**
Додаток збирає дані клієнтів?	Покупки / фінансова інформація / місцезнаходження / контактна інформація / контакти / вміст користувача / ідентифікатори / дані про використання / діагностика	Контактна інформація/ дані про використання/ діагностика (контактна інформація не надсилається при анонімному використанні)	Контактна інформація / ідентифікатори / дані про використання / діагностика	Ні
Дані користувача та/або метадані, надіслані материнській компанії та/або третім особам?	Так	Ні (додатковий номер мобільного телефону надіслано третій стороні для реєстрації)	Так	Ні
Шифрування ввімкнено за умовчанням?	Так (якщо пристрій це підтримує)	Так	Так	Так
Криптографічні примітиви	Curve25519 / AES-256 / HMAC-SHA256	ECDH512 / AES-256 / HMAC-SHA256	Curve25519 / ChaCha20 / HMAC-SHA256	X25519 / XSalsa20 256 / Poly1305
Чи програма та сервер повністю відкриті?	Ні	Ні	Так	Так

Продовження додатка 4

Критерії оцінки	Назва месенджера			
	Facebook Whatsapp	**Amazon Wickr Me**	**Wire**	**Session**
Чи використовуються відтворювані збірки для перевірки додатків на вихідний код?	Ні	Ні	Ні	Ні
Чи можете ви зареєструватися в програмі анонімно?	Ні	Так	Ні	Так
Чи можете ви додати контакт, не довіряючи серверу каталогів?	Ні	Ні	Ні	Так
Чи можете ви вручну перевірити відбитки пальців контактів?	Так	Так	Так	Так
Службу каталогів можна змінити, щоб увімкнути атаку MITM?	Так	Так	Так	Так
Чи отримуєте ви сповіщення про зміну відбитка пальця контакту?	Ні (параметр вимкнено за умовчанням)	Так	Так (якщо контакт був попередньо перевірений)	
Чи хешується особиста інформація (номер мобільного телефону, список контактів тощо)?	Ні	Так	Переважно	
Чи програма створює та зберігає закритий ключ на самому пристрої?	Так	Так	Так	Так
Чи може компанія читати повідомлення?	Так	Ні	Ні	Ні
Чи підтримує додаток повну секретність?	Так	Так	Так	Ні

Продовження додатка 4

Критерії оцінки	Назва месенджера			
	Facebook WhatsApp	**Amazon Wickr Me**	**Wire**	**Session**
Чи шифрує програма метадані?	Ні	Так	Переважно	Так
Чи використовує програма TLS/Noise для шифрування мережевого трафіку?	Так	Так	Так	Так
Чи використовує програма закріплення сертифіката?		Так	Так	Так
Чи шифрує програма дані на пристрої? (тільки для iOS і Android)		iOS: так (якщо ввімкнено парольну фразу); Android: так (невпевнений щодо функції)	Так	Так
Чи допускає програма вторинний фактор автентифікації?	Так	Так (використовується пароль для облікового запису)	Так	Так
Чи зашифровані повідомлення під час резервного копіювання в хмару?	iOS: так Android: так	Немає даних, Wickr виключено з резервних копій iCloud/iTunes і Android	Немає даних, Wire виключено з резервних копій iCloud/iTunes і Android	Немає даних, сеанс виключено з резервних копій iCloud/iTunes і Android
Чи реєструє компанія мітки часу/IP-адреси?	Так	Ні	Частково	Ні
Чи проводився нещодавно аудит коду та незалежний аналіз безпеки?	Ні	Так (серпень 2014)	Так (березень 2018)	Так (квітень 2021)
Чи добре задокументовано проект?	Частково	Частково	Частково	Частково

Додаток 5
до Методичних рекомендацій з питань забезпечення особистої кібербезпеки військовослужбовця (розділ 7)

Порівняння критеріїв оцінки веббраузерів Safari, Opera, Google Chrome

№ з/п	Критерії оцінки	Назва веббраузера		
		Safari	**Opera**	**Google Chrome**
1	**Поширеність**	Частка ринку – 14.45% Safari використовується на пристроях Apple і є браузером за умовчанням для macOS та iOS	Частка ринку – 5.31%. Дуже поширений, мультиплатформний, великий обсяг допоміжного та навчального матеріалу	Частка ринку – 61.1% Найбільш поширений, мультиплатформний, великий обсяг допоміжного та навчального матеріалу
2	**Продуктив-ність**	Швидкий та енергоефективний, особливо на пристроях Apple	Добра продуктивність, зосереджена на енергоефективності	Швидкий та ефективний, але може споживати багато ресурсів
3	**Безпека**	Відомий своїми суворими заходами безпеки, і Apple регулярно випускає оновлення для усунення вразливостей безпеки. Інтелектуальне запобігання відстеженню (ITP): функція допомагає захистити конфіденційність користувачів, обмежуючи можливість рекламодавців відстежувати користувачів на різних вебсайтах. Подібно до Chrome використовує ізольоване програмне середовище для ізоляції кожного вкладення та захисту системи від потенційних експлойтів	Підтримує стандартні налаштування безпеки. Заявлена наявність вбудованого VPN (фактично являє собою WEB proxy, який збирає та зберігає дані про діяльність користувачів, а не VPN)	Один з найбезпечніших. Кожне вкладення працює у власному процесі ізольованого програмного середовища, ізолюючи його від решти системи, що забезпечує додатковий рівень безпеки. Містить функцію безпечного перегляду, яка попереджає користувачів про потенційно небезпечні вебсайти та допомагає захистити від фішингу й атак зловмисного програмного забезпечення. Реалізує різні засоби для запобігання експлойтам для захисту від потенційних вразливостей і атак
4	**Конфіденцій-ність**	Може збирати більше даних користувачів порівняно з Firefox, Brave і Tor, особливо якщо користувачі ввійшли у відповідні облікові записи або підключилися до програм обміну даними	Найменш орієнтований на конфіденційність серед представлених	Може збирати більше даних користувачів порівняно з Firefox, Brave і Tor, особливо якщо користувачі ввійшли у відповідні облікові записи або підключилися до програм обміну даними

Продовження додатка 5

№ з/п	Критерії оцінки	Назва веббраузера		
		Safari 	**Opera** 	**Google Chrome** 
5	**Захист персональ-них даних**	Має надійні засоби безпеки для захисту облікових записів користувачів, таких як двофакторна автентифікація (2FA) і функції керування паролями	Може збирати, обробляти та використовувати дані користувача	Має надійні засоби безпеки для захисту облікових записів користувачів, таких як двофакторна автентифікація (2FA) і функції керування паролями
6	**Утиліти та інструменти**	Пропонують стандартні інструменти та утиліти перегляду, але можуть мати менше розширень/доповнень порівняно з Chrome і Firefox	Частка Opera на ринку порівняно з Chrome, Firefox та іншими основними браузерами невелика, що може вплинути на її розробку та бібліотеку розширень	Має величезну екосистему розширень, надбудов та інструментів розробника

Додаток 6
до Методичних рекомендацій з питань забезпечення особистої кібербезпеки військовослужбовця (розділ 7)

Порівняння критеріїв оцінки веббраузерів Mozilla Firefox, Microsoft Edge, Brave, Tor

№ з/п	Критерії оцінки	Назва веббраузера			
		Mozilla Firefox	**Microsoft Edge**	**Brave**	**Tor**
1	**Поширеність**	Частка ринку – 6.04% Дуже поширений, мультиплатформний має великий обсяг допоміжного та навчального матеріалу	Частка ринку – 10.77%. Дуже поширений, мультиплатформний, має великий обсяг допоміжного та навчального матеріалу. Є базовим браузером для сімейства ОС Windows	Не дуже поширений. Заснований на Chromium	Не дуже поширений. Заснований на Firefox
2	**Продуктив-ність**	Достатньо швидкий, але програє Google Chrome в базовій конфігурації. Може споживати значну кількість оперативної пам'яті	Швидкий, зі зменшеним споживання ресурсів. За подуктивністю близький до Google Chrome	Швидкий та ефективний, з фокусом на блокування реклами та трекерів	Швидкодія напряму залежить від сценарію використання та нод, що беруть участь у підключенні
3	**Безпека**	Містить розширений захист від відстеження, який за умовчанням блокує трекери сторонніх розробників і відомі шкідливі вебсайти, Використовує різні засоби пом'якшення експлойтів для захисту від потенційних загроз безпеці. Регулярно проходить незалежні аудити безпеки. Має великий досвід в оперативному вирішенні проблем безпеки	Edge на базі Chromium має ті самі функції безпеки, що й Chrome. Edge використовує Microsoft SmartScreen для захисту від спроб фішингу та шкідливих вебсайтів. Edge використовує технологію AppContainer для ізольованого програмного середовища окремих процесів, подібно до Chrome і Safari.	Brave розроблено з підходом до конфіденційності, блокує рекламу та трекери за умовчанням, забезпечуючи підвищену безпеку та конфіденційність. Brave Shields пропонує користувачам детальний контроль над дозволами вебсайтів, забезпечуючи додатковий захист від потенційних загроз. Примусове використання HTTPS протоколу та переадресація AMP посилань на оригінальні URL.	За умовчанням Tor Browser захищає вашу безпеку, шифруючи дані вебперегляду.

Продовження додатка 6

№ з/п	Критерії оцінки	Назва веббраузера			
		Mozilla Firefox	**Microsoft Edge**	**Brave**	**Tor**
4	**Конфіденційність**	Приділяє велику увагу конфіденційності. Має функцію захисту від відбитків пальців, щоб вебсайти не ідентифікували користувачів на основі конфігурації вебпереглядача.	Менш орієнтований на конфіденційність. Має базові функції, такі як режим конфіденційності та блокування відстеження	Браузер орієнтований на конфіденційність, який за умовчанням блокує рекламу та трекери, захищаючи користувачів від небажаного збору даних. Він також використовує функцію під назвою “Brave Shields” для блокування нав’язливого вмісту та підвищення конфіденційності	Створено для максимальної конфіденційності та анонімності, спрямовує трафік через глобальну мережу серверів, якими керують волонтер.
5	**Захист персональних даних**	Має надійні засоби безпеки для захисту облікових записів користувачів, таких як двофакторна автентифікація (2FA) і функції керування паролями	Має надійні засоби безпеки для захисту облікових записів користувачів, таких як двофакторна автентифікація (2FA) і функції керування паролями	Надає пріоритет захисту особистих даних і зменшенню відстеження користувачів	Надає пріоритет захисту особистих даних і зменшенню відстеження користувачів
6	**Утиліти та інструменти**	Має величезну екосистему розширень, надбудов та інструментів розробника	Має дещо меншу екосистему розширень, надбудов та інструментів, ніж Chrome та Firefox	Включає вбудоване блокування реклами, захист від відстеження та гаманець для криптовалют	Включає вбудоване блокування реклами, захист від відстеження, блокувальник скриптів
7	**Інше**	Firefox є браузером з відкритим вихідним кодом, і його код регулярно перевіряється експертами з безпеки та широким співтовариством розробників	Браузер від компанії Microsoft. Особливістю є можливість інтеграції з системою безпеки операційної системи Windows за допомогою Microsoft Defender Application Guard	Браузер з відкритим кодом	Браузер з відкритим кодом. Хоча браузер Tor забезпечує чудову анонімність, він не може запропонувати той самий рівень захисту від звичайних онлайн-загроз, які пропонують основні браузери, оскільки він зосереджений на анонімності.

Додаток 7
до Методичних рекомендацій з питань забезпечення особистої кібербезпеки військовослужбовця (розділ 7)

Порівняння критеріїв оцінки веббраузерів Librewolf, Mullvad, Vivaldi

№ з/п	Критерії оцінки	Назва веббраузера		
		Librewolf	**Mullvad**	**Vivaldi**
1	**Поширеність**	Не дуже поширений. Заснований на Firefox	Не дуже поширений. Спільний продукт з Tor Project	Не дуже поширений. Заснований на Chromium
2	**Продуктивність**	Спрямований на продуктивність та низьке споживання ресурсів	Швидкий та ефективний, з фокусом на приватність	Багатофункціональний інтерфейс Vivaldi може призвести до дещо нижчої продуктивності на пристроях нижчого класу
3	**Безпека**	Видаляє телеметрію, має схожий з Firefox перелік налаштувань безпеки	Має той самий рівень безпеки, що й Tor browser, але додатково шифрує трафік за допомогою VPN з'єднання	Функції безпеки такі ж, як і в інших сучасних браузерах, але його параметри налаштування та інструменти досвідченого користувача є більш широкими
4	**Конфіденційність**	Librewolf — це форк Firefox, орієнтований на конфіденційність, із додатковими налаштуваннями для покращення конфіденційності	Готові конфігурації та налаштування вебпереглядача маскують багато параметрів і функцій, які зазвичай використовуються для отримання інформації з пристрою. За умовчанням увімкнено приватний режим, який блокує трекери сторонніх розробників і файли cookie	Блокує сайти та рекламу, які можуть стежити за користувачем
5	**Захист персональних даних**	Надає пріоритет захисту особистих даних і зменшенню відстеження користувачів	Надає пріоритет захисту особистих даних і зменшенню відстеження користувачів	Надає пріоритет захисту особистих даних і зменшенню відстеження користувачів

Продовження додатка 7

№ з/п	Критерії оцінки	Назва веббраузера		
		Librewolf	**Mullvad**	**Vivaldi**
6	**Утиліти та інструменти**	Пропонує стандартні інструменти та утиліти перегляду, має менше розширень/доповнень порівняно з Chrome і Firefox	Основний інструмент – Mullvad VPN	Пропонує ряд вбудованих утиліт, включаючи розширене керування вкладеннями та функції швидкого доступу
7	**Інше**	Браузер з відкритим кодом. Librewolf, будучи форком Firefox, орієнтованим на конфіденційність, може мати меншу спільноту порівняно з основними браузерами, що може вплинути на оновлення та підтримку безпеки	Браузер з відкритим кодом. Фактично є тим самим Tor браузером, який замість децентралізованої мережі Tor використовує MullvadVPN	Налаштування за умовчанням досить далекі від забезпечення приватності. Обробка WebRTC Vivaldi за умовчанням залишає вас відкритими для експлойтів і витоків WebRTC, які можуть поставити під загрозу вашу конфіденційність

ПОСИЛАННЯ НА НОРМАТИВНО-ПРАВОВІ АКТИ ТА ВІЙСЬКОВІ ПУБЛІКАЦІЇ

Позначення нормативно-правового акта та ВП	Повне найменування нормативно-правового акта та військової публікації
1	2
	а. Закон України "Про основні засади забезпечення кібербезпеки України", із змінами, Верховна Рада України, Київ, 2020
	б. Закон України "Про телекомунікації", із змінами, Верховна Рада України, Київ, 2020
	в. Закон України "Про інформацію", із змінами, Верховна Рада України, Київ, 2016
	г. Закон України "Статут внутрішньої служби Збройних Сил України", затверджений № 548-XIV від 24.03.1999 (зі змінами та доповненнями Верховна Рада України)
	д. Наказ Міністерства оборони України від 28.12.2016 № 727 "Про затвердження Порядку використання мережі Інтернет у системі Міністерства оборони України"
	е. Пам'ятка "Щодо забезпечення інформаційної безпеки при роботі в мережі інтернет", Департамент контр-розвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, Київ, видання 2019
ВКП 18-00(01).01	**ж.** Доктрина "Публічного спілкування", затверджена Головнокомандувачем ЗС України 19.09.2020
ВП 1-185(49)03.01	**и.** Порадник "Медіаграмотність. Практичні поради військовослужбовцям Збройних Сил України", затверджений Головнокомандувачем ЗС України 27.07.2021
ТКП 3-116(01).01	**к.** Методичні рекомендації "З використання соціальних мереж у Збройних Силах України", затверджені Головнокомандувачем Збройних Сил України 01.09.2021
U/OO/155488-20 PP-20-0622	**л.** Info Sheet: "Mobile device best practices", October 2020 (Мобільні пристрої – найкращі практики захисту, видання жовтень 2020)
U/OO/166417-21 PP-21-1031	**м.** "CSI: Securing wireless devices in Public Settings", July 2021 (Інформаційний аркуш з кібербезпеки: Захист безпроводових пристроїв під час роботи в громадських місцях, видання липень, 2021)
U/OO/119184-23 PP-23-0270	**н.** "CSI: Best practices for securing your home network", February 2023 (Інформаційний аркуш з кібербезпеки: Найкращі практики для безпеки вашої домашньої мережі, видання лютий, 2023)

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

Скорочення та умовні позначення	Повне словосполучення та поняття, що скорочується
1	2
АНБ	Агентство Національної Безпеки Сполучених Штатів Америки
ЗС України	Збройні Сили України
ПЗ	Програмне забезпечення
США	Сполучені Штати Америки
ЦРУ	Центральне розвідувальне управління
Android	Операційна система
App Store	Платформа для пошуку і завантаження додатків/застосунків
DNS-фільтр	Domain Name System-фільтр (Механізм блокування доступу до певного контенту в Інтернеті)
Face ID	Сканер об’ємно-просторової форми людського обличчя
Google Play	Онлайн-магазин додатків/застосунків для операційної системи Android
GPS	Global Positioning System (Система глобального позиціонування)
HTTP	HyperText Transfer Protocol (Протокол передачі даних між користувацькими додатками/застосунками)
iCloud	Хмарне зберігання даних iOS Apple
iOS	Операційна система
IP-адреса	Ідентифікатор (унікальний числовий номер) пристроїв у мережі
MAC	Media Access Control address (Апаратна адреса пристрою)
PIN	Personal Identification Number (Персональний ідентифікаційний номер)
RCS	Rich Communication Services (Протокол передачі коротких повідомлень та контактних даних між абонентами мобільного зв’язку)
Touch ID	Сканер ідентифікації за відбитком пальця
VPN	Virtual Private Network (Віртуальна приватна мережа)
Wi-Fi	Wireless Fidelity (Бездротова правдивість відтворення)
ZIP-архів	Архівний формат, який стискає дані

1	2
NATO (НАТО)	North Atlantic Treaty Organization (Організація Північноатлантичного договору)
STANAG	Угода НАТО зі стандартизації

ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Аватарка – публічне графічне зображення особи, яке може бути довільною, документальною фотографією, чи фотографією, обробленою відповідно до побажань особи.

Автентифікація – електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних.

Акаунт або обліковий запис – віртуальний профіль користувача, до якого вносяться точні дані особистого кабінету. Це своєрідне електронне посвідчення особи, яке заповнюється для реєстрації та подальшого використання необхідних інтернет-ресурсів (сайтів комунальних підприємств, банківських установ, соціальних мереж, поштових сервісів, інтернет-магазинів, месенджерів тощо).

Буфер обміну – проміжне тимчасове сховище даних у межах операційної системи чи окремої програми, призначене для перенесення або копіювання тих чи інших даних.

Геопозиціонування – це процес визначення або оцінки географічного місцезнаходження об’єкта.

Геотегування – процес додавання географічних метаданих, що складаються з координат (широти та довготи), висоти, магнітного схилення та назв місцевості.

Двоетапна перевірка (двофакторна автентифікація) – це багаторівнева система безпеки для управління ідентифікацією та доступом, спрямована на захист вашого облікового запису.

Девайс – самостійний пристрій, який можна використовувати, “як є” (мобільний телефон, смартфон, планшет тощо).

Додаток – невелика програма, що доповнює і розширює функціональність основної програми.

Застосунок – прикладна програма, що дає змогу вирішувати певні задачі користувача.

Злам – дії або ряд сприятливих подій, спрямованих на створення порушення штатного режиму функціонування систем електронних комунікацій.

Конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом.

Лог – файл, у якому накопичується зібрана службова та статистична інформація про події в системі (програмі).

Месенджер – це додаток для миттєвого обміну текстовими повідомленнями, відеоматеріалами, відеодзвінками та голосовими дзвінками.

Оновлення ПЗ – це випущені розробником виправлення для програмного забезпечення, призначені для захисту та вдосконалення операційної системи, а також для захисту пристрою від вразливостей, пов’язаних із безпекою та конфіденційністю.

Операційна система – це базовий комплекс програм, що виконує керування апаратною складовою девайса та забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем

Платформа – це комплекс апаратних і програмних засобів, на якому функціонує програмне забезпечення користувача.

Повнодискове шифрування – вбудована функція шифрування для захисту даних. Передбачає введення пароля при кожному завантаженні мобільного пристрою.

Проксі-сервер – сервер, який виступає "посередником" між користувачем і цільовим сервером, забезпечуючи анонімний доступ до різних ресурсів, не розкриваючи при цьому інформації про походження запиту або користувача, щоб зловмисник не зміг визначити справжнє походження запиту.

Резервна копія – процес створення копії даних з пристрою зберігання (жорсткий диск, мобільний пристрій) і відновлення цих даних, якщо вони були пошкоджені або видалені.

Роутер – це мережевий пристрій, який з'єднує локальну мережу з Інтернетом і виконує такі функції: захищає локальну мережу від зовнішніх загроз; обмежує доступ користувачів локальної мережі до ресурсів інтернету; "роздає" IP-адреси; шифрує трафік.

Соціальна мережа – вебсайт або інша служба у Веб, яка дозволяє користувачам створювати публічну або напівпублічну анкету, складати список користувачів, з якими вони мають зв'язок та переглядати власний список зв'язків і списки інших користувачів.

Файли cookie – невеликі фрагменти тексту, що надсилаються у браузер з вебсайту, який ви відкрили, при цьому сайт запам'ятовує інформацію про здійснений візит.

Хост – технічний засіб/елемент інфраструктури мережі електронних комунікацій з доступом до IP-мережі, основне завдання якого – розподіл персональних даних та інформації із загальним доступом у вигляді листів, вебсайтів, блогів тощо.

Чат – програмне забезпечення/засіб обміну повідомленнями в реальному часі або близькому до нього.

Шифрування – це технічний процес, за допомогою якого інформація перетворюється на секретний код, маскуючи дані, які надсилаються, отримуються чи зберігаються.

Android – операційна система і платформа для мобільних телефонів та планшетних комп'ютерів, створена компанією Google на базі ядра Linux.

Google Диск – безпечне сховище для резервного копіювання файлів та роботи з ними на будь-яких пристроях.

iOS – це власницька мобільна операційна система від Apple. Розроблена спочатку для iPhone, згодом також вдосконалена для використання на iPad, iPod Touch та Apple TV.

Universal Plug And Play (UPnP) – універсальне автоматичне налаштування мережевих пристроїв.

Цитата (*citation, від лат. cito – зрушую, викликаю*) – порівняно короткий уривок з літературного, наукового чи будь-якого іншого опублікованого твору, який використовується, з обов'язковим посиланням на його автора і джерела цитування, іншою особою у своєму творі з метою зробити зрозумілішим свої твердження або для посилання на погляди іншого автора в автентичному формулюванні [1].

Інші терміни, які використовуються у цих Методичних рекомендаціях, вживаються у значеннях, наведених, Методичні рекомендації "З використання соціальних мереж у Збройних Силах України", затверджені Головнокомандувачем Збройних Сил України 01.09.2021 (посилання **к**) та інших нормативно-правових актах України (посилання **а – г**), Міністерства оборони України (посилання **д, е**) та Генерального штабу ЗС України (посилання **ж, и**).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ (ДЖЕРЕЛ)

1. Закон України “Про авторське право і суміжні права” в редакції закону України від 11.07.2001 № 227-III.

2. Порядок оформлення військових публікацій у Збройних Силах України, ДДП 1-0(189), затверджені наказом Головнокомандувача Збройних Сил України 19 лютого 2022 року № 60.

3. Інструкція зі зберігання і користування особовим складом ЗС України засобами стільникового зв’язку та іншими електронними засобами, затверджена та введена в дію наказом Головнокомандувача ЗС України від 01.07.2020 № 74.

ДЛЯ ЗАМІТОК

ДЛЯ ЗАМІТОК