ЗМІСТ

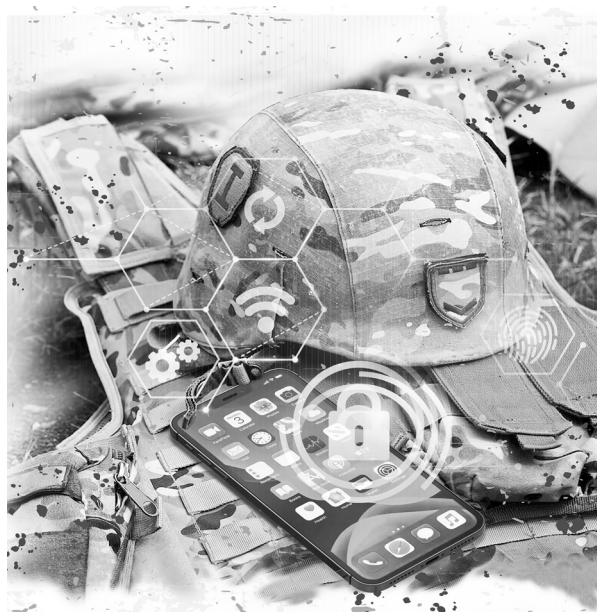
Забезпечення особистої кібербезпеки військовослужбовця

Анотація

Ця публікація розроблена 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).

ЗАБЕЗПЕЧЕННЯ ОСОБИСТОЇ КІБЕРБЕЗПЕКИ ВІЙСЬКОВОСЛУЖБОВЦЯ



МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

Видавництво
«Центр учбової літератури»
Київ – 2023

УДК 316.77:004.738.5(477)
3-12

Забезпечення особистої кібербезпеки військовослужбовця: методичні
З-12 рекомендації / В. Докіль, Ю. Кисленко, Є.Живило, Ю.Бондаренко, М. Краснощок, К. Кравченко. — Київ: «Центр учбової літератури», 2023. — 62 с.

ISBN 978-611-01-2945-9

Ця публікація розроблена 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).

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.

ISBN 978-611-01-2945-9

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

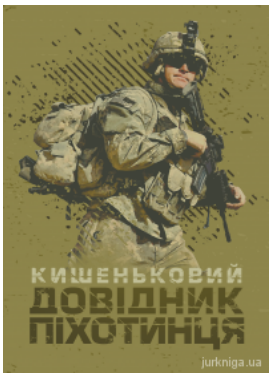
У наш час найпоширенішими месенджерами є Signal, Telegram, Viber, WhatsApp, Facebook Messenger. Використання двофакторної автентифікації допоможе уберегти себе від перехоплення зловмисником контролю над вашим обліковим записом. Нижче наведено порядок активації двофакторної автентифікації, а також загрози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

Книги, які можуть вас зацікавити



Кишеньковий довідник піхотинця

Боротьба з ударними БпЛА іранського та російського виробництва «Shahed-136» («Герань-2») та «Ланцет-2». Методичні рекомендації загальновійськовим...

Организация противодействия малым БПЛА. Книга ворога ворожою мовою

Сугестивні технології маніпулятивного впливу

Мислення розвідника. Як припинити обманювати себе й побачити найкраще рішення

Лінії радіозв'язку та антенні пристрої

Перейти до галузі права
Військове право