СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Практичні рекомендації з кібербезпеки під час ведення бойових дій

Зміст:

Безпека мобільного телефону

Загальні рекомендації

Війна ведеться не тільки на полі бою, але і в Інтернеті. Знайте, що в мережі Ваші необережні дії можуть привести ворожих особ не тільки до ваших побратимів, але й до вашої родини, батьків чи близьких.

Перш за все, необхідно знати, що порядок користування військовослужбовцями мобільними телефонами та іншими електронними засобами визначає командир військової частини (стаття 143 Статуту внутрішньої служби Збройних Сил України). Тобто командир приймає рішення і визначає, коли, як і де можна здійснювати дзвінки.

Не використовуйте мобільний телефон в зоні ведення бойових дій без нагальної потреби, а за можливості - використовуйте мережі визначеного, безпечного, службового зв'язку.

Не зберігайте на телефоні фото, відео, документів та будь-якої іншої інформації, яка може бути використана у випадку втрати гаджету і потрапляння його до рук ворога. Опрацювали отриману інформацію - видаліть її повністю.

Якщо ви придбали вживаний телефон, то перепрошийте його повністю у довіренному сервісному центрі, щоб стерти можливі віруси та шкідливі програми від минулого власника.

Фізична безпека

Ваш телефон - це ваша особиста річ. Не дозволяйте його використання без вашого дозволу та без спостереження за діями використовувача.

Встановіть надійний пароль розблокування не менш ніж з 6 цифр, або цифро-літерний пароль. Не використовуйте розповсюджені паролі, типу: 111111, 123321, qwerty.

Налаштуйте автоблокування телефону в найкоротший термін (1-5 хв).

Налаштуйте видалення даних або повне блокування після 5 невдалих спроб вводу пароля.

Не використовуйте графічний ключ та розблокування обличчям (крім Face ID в iPhone). Це не надійний захист.

Не підключайте до телефону чужих сім-карт, карт пам'яті, флешок, павербанків, шнурів, зарядних пристроїв та інших речей, походження яких має сумніви. Ці речі можуть як заразити ваш телефон вірусами, так і фізично знищити його.

Не використовуйте телефон, як флешку для переносу інформації з комп'ютера. Придбайте в надійному магазині для цього окремий пристрій. У продажі є флешки, з двома USB портами: для комп'ютера та телефона.

Програмна безпека

Геолокація

В налаштуваннях телефону - вимкніть служби геолокації та вмикайте їх тільки тоді, коли ви збираєтесь ними користуватись (для мап, для польотів на дроні).

Подивіться, яким додаткам надані права на користування геолокацією, вимкніть її для тих, кому вона не потрібна для роботи. Наприклад: камера, месенджери, калькулятор, ігри тощо.

Android

Ніколи не встановлюйте root на свій телефон.

Зареєструйте новий Google аккаунт на новий номер, використовуючи стійкий пароль (див. розділ "Надійні паролі" нижче). Налаштуйте двофакторну аутентифікацію та інші налаштування приватності.

Встановлюйте додатки ЛИШЕ з офіційного Play Market. За винятком тих, що були розроблені для ЗСУ та розповсюджуються фахівцями підрозділу.

Не встановлюйте додатки, у яких розробники з росії (Yandex, Mail.ru, VK, Одноклассники та ін. непотріб).

Не встановлюйте додатки, які пересилають в месенджерах або електронною поштою. Якщо додаток прийшов від фахівця підрозділу - впевнитись, чи дійсно він його мав надіслати.

Видаліть з телефону все зайве, що не потрібно для виконання завдань.

Встановлюючи додаток, звертайте увагу до чого додаток питає доступ. Не надавайте доступи, якщо це викликає у вас підозру.

Оминайте додатки, які "видаляють віруси", "чистять пам'ять" чи "прискорюють телефон". Не встановлюйте "зламані" ігри. В більшості випадків - це шкідливе п\з яке буде просто з'їдати ресурси телефону або заразить його вірусами.

Уникайте "кастомних прошивок" для телефонів.

Чим більш популярна програма в маркеті - тим вона менш небезпечна. Звертайте увагу на кількість інсталяцій (сотні тисяч) та відгуки.

iPhone

Телефони цієї марки більш захищені та краще відповідають сьогоденним вимогам безпеки. Гарним вибором будуть моделі від iPhone X та новіші через їх просунуту безпеку та функцію Face ID. Надійний пароль на телефон та iCloud - захистять вас від багатьох проблем.

Мінусом буде те, що деякі додатки, які використовуються військовими будуть недоступні для цієї платформи.

Для більшої безпеки можна встановити системні паролі на застосунки, які зберігають приватну інформацію (галерея, месенджери, соціальні мережі):

1. Активуйте функцію «Екранний час» у відповідному підпункті меню «Налаштування»;
2. Натисніть на сенсорну кнопку «Використовувати код-пароль» і введіть будь-яку відому лише вам послідовність символів;
3. Торкніться графіка статистики використання програм на вашому пристрої та

виберіть потрібну програму зі списку;

У самому низу екрана розташовуватиметься «кнопка» з написом «Додати ліміт». Необхідно її натиснути та встановити час, наприклад 1 хвилину. Після цього достатньо активувати тумблер навпроти пункту Блокувати в кінці списку.

Після закінчення встановленого часу (у прикладі однієї хвилини) програма заблокується. Для його розблокування достатньо натиснути на кнопку «Ігнорувати ліміт» і ввести вибраний при налаштуванні пароль.

VPN та Tor

Використання VPN допомагає вам приховати та додатково зашифрувати Інтернет трафік з вашого мобільного чи комп'ютера.

VPN варто використовувати для усього Інтернет-трафіку а не тільки для браузера.

Платний VPN від таких постачальників як Proton VPN, NordVPN, Pure, ExpressVPN, Cyberghost, SurfShark вважаються найнадійнішими. Майже в усіх є безкоштовний пакет з лімітованими можливостями.

Повністю безкоштовною альтернативою для перегляду сайтів буде використання браузера Tor, але крім iPhone - там він платний.

В iPhone за мінімальний пакет iCloud в 0.99$ буде доступний вбудований VPN від Apple, який убезпечить серфінг в Інтернеті та приватність електронної пошти.

Інструкцію з налаштування VPN на вашому телефоні можна прочитати у відповідному розділу на обраному сервісі або знайти в інтернеті.

Безпека месенджерів

Загальні рекомендації

- Приберіть із налаштувань або закрийте для загалу усю особисту інформацію
  - Номер телефону (також перереєструйтесь, використовуючи службову сім-картку);
  - Дату народження;
  - Інформацію в профілі про місце проживання, місце роботи, посаду, військову частину, рід військ тощо;
  - Аватари з відкритим лицем;
  - Ім'я та ім'я акаунту замініть на нейтральне;
- Не поширюйте фото, відео, за якими можна ідентифікувати ваше місцерозташування. Не поширюйте фото техніки, позицій тощо;
- Не додавайте у друзі чи в контакти сторонніх, невідомих вам осіб;
- Упевніться що людина, з якою ви ведете розмову, не видає себе за когось іншого.
- Не відкривайте файлів та посилань від незнайомців (і навіть від друзів чи рідних, якщо надіслане викликає сумніви);
- Відключіть можливість бачити вашу останню активність, а також – надсилати вам повідомлення для акаунтів, що не належать до переліку контактів;
- Використовуйте для спілкування чати з наскрізним шифруванням;
- Налаштуйте зникаючі повідомлення на 7 днів або меньше у кожному месенджері

Facebook Messenger

Як включити наскрізне шифрування у Facebook Messenger:

- Перейдіть до профілю користувача. Це можна зробити, вибравши чат, який ви маєте з ними, і натиснувши зображення профілю.
- У розділі «Інші дії» виберіть «Перейти до секретної розмови», а потім почніть переписку

Як включити двофакторну аутентифікацію у Facebook Messenger:

- Відкрийте настройки безпеки та авторизації у Facebook.
- Перейдіть до розділу Використати двофакторну автентифікацію та натисніть Редагувати.
- Виберіть потрібний спосіб перевірки та дотримуйтесь інструкцій на екрані.

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

- Ключ безпеки на сумісному пристрої.
- Коди для входу, що генеруються стороннім додатком для автентифікації.
- Коди у SMS, що надходять на мобільний телефон

Використання електронної пошти

Безпека електронної пошти - це другий по важливості, після мобільного номеру, фактор вашої безпеки.

Атаки направленні на пошту - найрозповсюджені та найнебезпечніші. Від підключення вас до кругових спам розсилок до отримання доступу к інформації на пристрої або виведення його з ладу. Приділяйте увагу безпеці електронного листування.

Розділяйте поняття «службові» та «особисті» потреби під час використання електронної пошти.

Не використовуйте свою поштову скриньку на ресурсах gov.ua (відкрита службова скринька) для реєстрації в соціальних мережах, форумах чи розважальних сайтах. Службова поштова скринька повинна використовуватися виключно у СЛУЖБОВИХ цілях, а не для листування з друзями.

Безпечні поштові сервісі це Gmail, iCloud, Proton та ukr.net. Перший з них - найбезпечніший та рекомендується для першочергового використання.

Для різних поштових скриньок - різні надійні паролі. Не використовуйте однакові паролі на всіх поштових сервісах.

Не натискайте на посилання і прикріплені файли, отримані в листі, якщо його вміст або адресат викликає підозру (звертайте увагу на яку адресу веде посилання). Часто противник або зловмисник, який знає вашу пошту, може сформувати фейковий лист від нібито існуючої людини чи відділу. Наприклад, про нарахування премії або відпустки. Якщо маєте сумніви щодо автора чи вмісту листа, зв'яжіться з відправником іншими засобами зв'язку та уточніть час відправлення, назву та розмір відправленого файла (адресу посилання, кількість фото тощо). Якщо щось не збігається, НЕГАЙНО надайте доповідь керівнику і спеціалістам з

кібербезпеки. Такі атаки, зазвичай, здійснюються масованими розсилками подібних листів, тому оперативність реагування відіграє визначальну роль у протидії зловмисникам.

Безпека веб-браузера

Безпечними браузерами вважаються: Safari (iOS), Tor (Android), Chrome та Mozilla Firefox (усі платформи). Не використовуйте інші браузера та видаліть їх, якщо вони у вас встановлені.

В звичайному режимі можна відвідувати ті сайти, яким ви точно довіряєте та заходите по прямій адресі. Для пошуку нової інформації - використовуйте режим інкогніто.

Звертайте увагу, щоб з'єднання з сайтом було захищене. Якщо браузер починає присилати сповіщення щодо сертифікатів чи небезпечного з'єднання - припиніть використання браузера негайно та закрийте його.

Порнографічний контент в Інтернеті - це найкоротший шлях до компрометації вашої безпеки. Не шукайте та не переходьте по оголошенням, вспливаючим вікнам, електронним листам чи повідомленням у мессенджерах з таким змістом.

Безпека персонального комп'ютера

Загальні рекомендації

Завжди дотримуйтесь вимог чинних наказів та інструкцій, які стосуються користування персональними комп'ютерами, навіть при користуванні особистим ПК у службових цілях.

Ваш комп'ютер - це ваша особиста річ. Контролюйте доступ до нього.

Надайте перевагу використанню ПК з операційною системою на базі ядра Linux (програмне забезпечення Ubuntu*Pack (UALinux) має експертний висновок ДССЗЗІ України).

Заборонено обробляти службову та секретну інформацію на особистих комп'ютерах. ПК, на яких опрацьовуються документи з обмеженим доступом заборонено мати доступ до мережі Інтернет, в тому числі для всіх програм (за допомогою налаштувань Windows Defender Firewall, щоб навіть у випадку фізичного з'єднання ПК з мережею Інтернет (через модем, тощо), не сталося витоку інформації. На зазначених ПК, у разі наявності, фізично та програмно вимкнути модулі бездротових підключень (WiFi).

При підключенні до Інтернету - надавайте перевагу кабельному підключенню, як більш надійному. Бездротове підключення має бути захищено стійким паролем та використовувати WPA2 без WPS.

Не підключайте до комп'ютера флешок, кабелів, периферії яка має сумнівне походження. Використовуйте лише обліковані носії інформації в межах свого підрозділу. Пам'ятайте, що кожен носій має свій «гриф». Не використовуй у службових цілях сторонні носії інформації, особливо особисті. Не користуйся обліковаными носіями в особистих цілях.

Не зберігайте відскановані копії особистих та службових документів на комп'ютері та у хмарних сховищах (Dropbox, Google Drive тощо), на пошті чи у відкритих мережевих папках у комп'ютері.

Зараження комп'ютера вірусом може мати непередбачувані наслідки для вашої безпеки та безпеки вашого підрозділу. Робіть усе можливе, щоб не допустити зараження.

Антивірусне програмне забезпечення

Встановіть антивірус та не перешкоджайте скануванню комп'ютера. Держспецзв'язку схвалює: Avast, ESET, McAfee, Zillya.

Регулярно оновлюйте антивірусну базу, наприклад з сайту https://cazi.gov.ua/. В таких базах міститься інформація про нові загрози, небезпечні файли та шкідливий код. Це правило особливо важливе для безкоштовних версій антивірусів.

Завантажуйте антивірус та програми, якими користуєтеся, тільки з офіційного сайту розробника чи з перевірених джерел.

Налаштуйте автоматичне сканування загроз при підключенні зовнішніх носіїв. Вимкніть автовідтворення для всіх носіїв та пристроїв.

Першочергові дії у випадку підозрілої активності або виявлення ШПЗ на ПК:

1. Терміново зверніться до адміністратору підрозділу.

2. Ізолювати ПК (відключити доступ до мережі Інтернет для недопущення розповсюдження та подальшої активності ШПЗ).

3. Оновити сигнатурну базу АВПЗ на ураженому ПК (завантажити офлайн оновлення) та запустити сканування.

4. У разі неможливості використання АВПЗ ESET на ПК, завантажити безкоштовний сканер "Microsoft Safety Scanner" (https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download?view=o365-worldwide) та виконати сканування.

5. Перевірити (просканувати) флеш носії та диски, що взаємодіяли з ураженим ПК на наявність підозрілих файлів (звернути увагу на приховані файли).

6. Після перевірки всіх файлів потенційно ураженого ПК, локалізації та видалення шкідливих файлів, рекомендовано, у разі необхідності, перевстановити операційну систему.

Системні рекомендації

Завжди тримайте систему оновленою. Замініть Windows XP та Windows 7 на Windows 10 з актуальними оновленнями ПЗ. Де це неможливо - ізолюйте ПК від мережі Інтернет та своєчасно оновлюйте антивірус.

Встановіть надійний пароль на вхід у систему та блокування входу після 5 невдалих спроб.

Створіть окремий обліковий запис в системі з найнижчими правами (гість) та працюйте з під нього. Не працюйте з облікового запису з правами адміністратора. Обов'язково встановіть різні надійні паролі на обидва акаунти.

Для гостя має бути обмежено:
- запуск PowerShell, CMD, wscript.exe;
- редагування правил Windows Defender Firewall, реєстру;
- вимкнення АВПЗ або редагування файлів його конфігурації.

Кожна вищезазначена дія та установка будь-якого ПЗ на ПК має проводитись виключно під обліковим записом адміністратора.

Вимкніть можливість запуску макросів в документах Microsoft Office. Параметри - Центр безпеки - Параметри макросів - Вимкнути всі макроси зі сповіщенням.

Регулярно перевіряйте Task Scheduler та автозапуск на наявність підозрілих скриптів, які запускаються з директорій користувача. Для цього можна використовувати утіліту CCleaner. В той же час, інформація щодо надійності цього програмного засобу – відсутня.

В налаштуваннях Windows Defender Firewall створити правила, які забороняють вихід в мережу Інтернет програм: powershell.exe, wscript.exe, cmd.exe, word.exe. Рекомендовано надати доступ до мережі Інтернет лише тим програмам, яким це необхідно (браузери, поштові клієнти, система "Кропива" та іншим), а всім іншим програмам - заборонити.

Не використовуйте піратське ПЗ! Пошукайте альтернативні програми серед програмного забезпечення у вільному доступі (наприклад, Libre Office замість MS Office) або придбайте

ліцензійну копію.

Якщо ваша кваліфікація дозволяє, то використовуйте Linux-систему з встановленою віртуальною машиною на Windows. Це дозволить ізолювати загрози усередині "пісочниці".

Зашифруйте вашу систему за допомогою вбудованих засобів (Windows BitLocker та Device Encryption) або утиліти VeraCrypt. Це майже унеможливить доступ до інформації на комп'ютері у разі фізичного доступу до ПК ворога.

Створіть файловий контейнер VeraCrypt для зберігання чутливої та секретної інформації.

Створіть зашифрований розділ на USB-носії для переносу важливої інформації між комп'ютерами - це зменшить вірогідність попадання інформації до ворожих осіб при втраті носія.

Соціальна інженерія та анонімність

Для воєнного часу, краще створити собі нову віртуальну особистість, а старі соц. мережі почистити від зайвої інформації та закрити від публічності. Спробуйте застосувати правила нижче до існуючих акаунтів та ускладніть ворогу збір інформації про вас.

Створіть нову поштову скриньку на сервісі Gmail, з новим надійним паролем. Налаштуйте двофакторну аутентифікацію та перевірте налаштування безпеки акаунта.

Не використовуйте назви свого підрозділу, ім'я, прізвища, військові псевдо та нікнейми з цивільного життя для:

- Назв поштових скриньок
- Акаунтів у соц. мережах та месенджерах
- Паролях

Не розкривайте персональної інформації

Перше, на що звертають увагу розвідники — це ваш профіль у соцмережі. З аватарки (зображення користувача), дати народження, роду занять і груп, у яких зареєстрований користувач, зрозуміло, чим живе і займається та чи інша людина. Наприклад, якщо в розділі про освіту значиться, що в 2013 році особа закінчила Львівську академію Сухопутних військ, у переліку груп «72 Гвардійська омбр», а на фото багато БМП, то майже точно можна сказати, що це старший лейтенант, командир взводу в 72 омбр. А більш глибокий аналіз номерів техніки чи окремих осіб на фото розкриє батальйон, роту і, можливо, навіть взвод, яким особа командує. У середньому, досвідченому співробітнику достатньо дві-три хвилини, щоб оцінити «корисність» цілі. Загалом, ці дві хвилини найбільш важливі, оскільки показавши, що ви військовий, постійно або періодично перебуваєте в зоні бойових дій, маєте велике коло знайомств серед військовослужбовців та волонтерів, то ви стаєте потенційною ціллю кібератак та розвідспрямувань.

Тим не менше, достатньо не надавати реальної інформації про себе або надавати її частково. Для цього в розділі «Налаштування приватності» треба зробити певні корегування:

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

У всіх соцмережах можна розділяти друзів по групах. Створіть спеціальну групу для «ненадійних друзів» (яких ви не знаєте у реальному житті) та обмежте їх права на рівні звичайних користувачів;

Закрийте можливість перегляду фото та відеоматеріалів усім користувачам, окрім друзів;

Не надавайте інформації про місце роботи/служби, рік закінчення школи, вузу тощо.

Налаштувавши таким чином доступ до своєї сторінки, всі, окрім друзів, бачитимуть лише ваше ім'я, фото та інформацію, якою ви поділилися на своїй сторінці. Швидше за все таку сторінку проігнорують або просто не стануть морочитися із закритою сторінкою, коли в мережі повно відкритих. Крім цього, досить ефективним способом приховати дані про себе та не стати «донором» розвідданих є дезінформація. Псевдо, написане латиницею, на аватарці фото якоїсь квітки та вища освіта, отримана в Черкаському інституті рослинництва та легкої промисловості в 1994 році, навряд чи дадуть підстави думати, що це сторінка старшого лейтенанта з «сімдесятдвійки».

Важливо. *Відповідно до Федерального закону рф «Об информации, информационных технологиях и о защите информации» з поправками від 5 травня 2014 року, на всі сайти, сторінки чи блоги з відвідуваністю понад 3 тис. користувачів за добу накладаються певні обмеження. Тепер власники цих ресурсів повинні зберігати дані користувачів на території рф для надання її, в разі потреби, Роскомнагляду чи спецслужбам. Іншими словами, вся інформація з профілю, включаючи особисте листування, фото та відео в соціальних мережах і сервісах з позначкою .ru, буде передана відповідним службам на підставі одного-єдиного запиту. Безпечніше використовувати Facebook і Twitter, ніж «ВКонтакте» і «Одноклассники».*

Завантажуючи фото, пам'ятайте про небезпеку

Основним джерелом інформації із соцмереж є фотографії. Мабуть, мало в Україні людей, які не бачили матеріали від *InformNapalm* — української групи розвідки з відкритих джерел, що, переважно, спеціалізується на розслідуваннях та документуванні злочинів РФ в Україні. За два роки війни сотні терабайт інформації що містять досьє на бойовиків, було зібрано з мережі, переважно, з фотографій та відео, завантажених у соцмережі.

Метадані фотографій можуть містити інформацію про дату, час знімка, геолокацію та пристрій з якого зроблене фото.

Потрібно вимкнути геотегінг або геопозиціонування. Багато телефонів за стандартними налаштуваннями самостійно прикріплюють до фото службову інформацію, яка вказує на місце і час знімка. Цінність і небезпечність такої інформації за два роки бойових дій уже всі усвідомили. Тож необхідно обов'язково перевірити та вимкнути це налаштування;

Важливо. *Міжнародна група цивільних журналістів Bellingcat встановила, що зенітно-ракетний комплекс «Бук», за допомогою якого було збито Боїнг-777 Малазійських авіаліній МН-17, входив до складу 53-ї зенітно-ракетної бригади, що базується в Курській області. Висновки зроблено на підставі фото- та відеоматеріалів з мережі Інтернет. Ідентифікацію конкретної установки було здійснено шляхом аналізу семи його відмінних рис, у тому числі характерної вм'ятини на пластині лівого борту, білих відміток на шасі і комбінації підключення кабелів до лафета пускового пристрою.*

Тому, пересилаючи фото, або викладаючи будь які зображення до соціальних мереж проаналізуйте що саме зображено на фото, або на фоні чого сфотографовано об'єкт.

Надійні паролі

13 ознак надійного пароля:

1. У паролі — понад вісім символів.
2. Він не містить символів, що повторюються або йдуть один за одним (0000, 1111,