СЛУЖБА БЕЗПЕКИ УКРАЇНИ

ДЕПАРТАМЕНТ
КОНТРРОЗВІДУВАЛЬНОГО ЗАХИСТУ
ІНТЕРЕСІВ ДЕРЖАВИ У СФЕРІ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ПАМ'ЯТКА
ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОБОТІ В МЕРЕЖІ ІНТЕРНЕТ

м. Київ
2020 рік

Перелік основних чинників, що впливають на стан інформаційної безпеки у зв'язку із використанням загальнодоступних та соціально-орієнтованих ресурсів мережі Інтернет

- *Військова агресія Російської Федерації та пов'язані з нею масштабні кібератаки, масові антиукраїнські інформаційні кампанії та їх психологічний вплив на користувачів українського сегменту мережі Інтернет, отримання несанкціонованого доступу до персональних даних та іншої важливої інформації з електронних поштових скриньок та соціальних мереж тощо.*
- *Існування загрози для державних установ (міністерств, відомств, агентств, фінансових установ тощо) у зв'язку із використанням працівниками у службовій діяльності програмного забезпечення російського виробництва, а також поштових електронних сервісів, соціальних мереж «ВКонтакте» та «Одноклассники», доступ до яких на даний час обмежено відповідно до Указу Президента України № 184/2020 від 14.05.2020 року.*
- *Підконтрольність найбільших та найвпливовіших медіа особам, які використовують вказані ресурси для лобіювання та відстоювання особистих, а не державних інтересів.*
- *Активне наповнення соціальних мереж замовними дописами відповідного контенту із використанням т.зв. бот-мереж («ботів»), технології масового «тролінгу» та таргетингової реклами.*
- *Маніпуляції у засобах масової інформації та соціальних мережах з метою привернення уваги більшої аудиторії шляхом використання методів соціальної інженерії.*
- *Використання соціальних мереж для поширення недостовірної (фейкової), викривленої, деструктивної інформації та здійснення маніпулятивного впливу на суспільну свідомість користувачів українського сегменту мережі Інтернет.*

Характеристика ключових факторів ризику та рекомендації щодо їх нейтралізації

1. Зберігання та передача даних

Недотримання окремих правил безпеки під час здійснення службових обов'язків працівниками органів виконавчої влади та місцевого самоврядування, посадовими особами державних підприємств, установ, організацій може призвести до втрати чи

крадіжки мобільних телефонів, персональних ноутбуків, магнітних носіїв інформації тощо. Вказане ставить під загрозу збереження персональних даних та може призвести до розголошення інформації з обмеженим доступом.

Порушення базових вимог законодавства про захист інформації в інформаційно-телекомунікаційних системах *(далі – ІТС)*, що створюють сприятливі умови для реалізації кіберзагроз, які полягають у:

- *здійсненні несанкціонованого доступу до баз даних;*
- *копіюванні та передачі через незахищений канал мережі Інтернет документальних матеріалів, що містять службову інформацію;*
- *використанні особистих технічних засобів у складі виробничих автоматизованих систем (USB-флеш накопичувачі);*
- *підключенні до комп'ютерних систем технічних засобів із модулями передачі даних (Bluetooth, GSM тощо), призначених для створення каналів зв'язку з мережами загального користування та іншими електронними пристроями;*
- *незахищеності ІТС за допомогою актуальних версій антивірусного програмного забезпечення.*

З метою уникнення негативних наслідків у випадку втрати або викрадення носіїв інформації необхідно:

- *встановити паролі на усі пристрої, що перебувають у користуванні (PIN-коди, паролі на доступ до всіх облікових записів, паролі на планшетах та ноутбуках тощо);*
- *систематично робити резервне копіювання важливих файлів;*
- *блокувати пристрої щоразу після закінчення роботи з ними.*

2. Соціальні мережі

Соціальні мережі у наш час стали зручним та ефективним засобом комунікації. За допомогою соціальних медіа можна обмінюватись повідомленнями, публікувати особисті фото- та відеоматеріали, розміщувати інформацію про місце роботи і відпочинку, колег, друзів, навчання, дозвілля, політичні погляди тощо. Така кількість приватної інформації у разі її потрапляння до зацікавлених осіб може поставити під загрозу як службову діяльність так і приватне життя держслужбовців, керівників підприємств, установи, організації, працівників органів виконавчої влади та місцевого самоврядування.

З метою уникнення несанкціонованого доступу до персональних акаунтів, зареєстрованих у соціально-орієнтованих ресурсах мережі Інтернет, необхідно:

•встановити надійний пароль для доступу у обліковий запис. При цьому, рівень захищеності акаунту та інформації, що знаходиться в ньому, залежить від складності встановленого паролю;

•використовувати функцію подвійної авторизації. Щоб увійти до профілю з незнайомого пристрою, сервіс вимагатиме пройти додаткову ідентифікацію як власника акаунту. При цьому, на вказаний номер телефону або на поштову скриньку буде надіслано повідомлення з кодом підтвердження, або необхідно буде ввести один із паролів, які попередньо були збережені через інший обраний спосіб підтвердження;

•здійснити додаткові налаштування профілю в соціальних мережах з метою отримання інформації щодо несанкціонованого доступу до ресурсів з невідомого пристрою або Інтернет-браузера;

•при створенні акаунтів у соціальних мережах використовувати у якості логіна поштову адресу надійного сервісу (наприклад «Google», «Yahoo»), або українських поштових сервісів. Не рекомендується користуватися російськими сервісами, доступ до яких заборонено в Україні, оскільки через персональну електронну скриньку можна отримати пароль, а відтак доступ до профілів, зареєстрованих у соціальних мережах;

*•**не здійснювати** авторизацію особистих чи робочих, корпоративних профілів з незнайомих чи незахищених пристроїв. Існує ймовірність, що після завершення роботи не буде здійснено вихід із облікового запису або пристрій запам'ятає вказаний при вході логін та пароль. Крім того, існує ймовірність ураження такого пристрою шкідливим програмним забезпеченням, що може здійснювати збір та передачу відомостей щодо паролів та логінів зацікавленим особам;*

*•**не відкривати** вкладень у підозрілих повідомленнях від адресатів щодо яких виникають сумніви;*

*•**пам'ятайте**, що саме фішинг (довідково: **фішинг** – вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі Інтернет персональних даних клієнтів, сервісів із переказу або обміну валюти, Інтернет-магазинів) є найпоширенішим способом отримання зловмисниками паролів до поштових скриньок та сторінок у соціальних мережах.*

Крім того, у ході гібридної агресії з боку РФ соціальні мережі активно використовуються для збору додаткових відомостей щодо місць регулярного перебування особи, її родичів, колег, особистих уподобань та іншої приватної інформації. Водночас, через соцмережі здійснюється збір та передача інформації щодо місць дислокації та складу окремих підрозділів Збройних сил України, які залучені до проведення операції об'єднаних сил на сході України.

З метою недопущення отримання зацікавленими особами додаткової (приватної) інформації стосовно особи, членів її сім'ї, колег:

• ***не публікувати*** *у соціальних мережах інформацію, що може поставити під загрозу особисте життя особи, життя членів її сім'ї та інших осіб;*

• *членам сімей військовослужбовців не варто публікувати фото- та відеоматеріали, за допомогою яких можна визначити їх місцезнаходження, отримати дані про озброєння та діяльність військової частини, окремих збройних військових формувань, що беруть участь у проведенні операції об'єднаних сил на сході України. Вказані дії можуть загрожувати життю та здоров'ю людей, а також створює передумови до вербувальної діяльності спеціальних служб іноземних держав, насамперед Російської Федерації;*

• *обмежити доступ до приватної інформації в налаштуваннях конфіденційності соціальної мережі. Вибрати налаштування, які найбільше захищають додаткові відомості про власника акаунта. Зокрема,* ***не зазначати*** *геолокацію (місце розташування);*

• *періодично переглядати список «друзів» у соціальній мережі. Якщо серед них є незнайомі або підозрілі акаунти, необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу. У подальшому необхідно бути уважними під час додавання до списку «друзів» нових користувачів;*

• ***не рекомендується*** *використовувати російські соціальні мережі «ВКонтакте», «Одноклассники» та «Linkdelin», а також месенджер «Qip» (у т.ч. із застосуванням сервісів VPN), а також використання російських пошукових систем «Mail.ru» та «Yandex», доступ до яких заборонено, оскільки останні на вимогу спецслужб РФ можуть передавати відомості щодо персональних даних власників акаунтів (e-mail, номер мобільного телефону, дата та IP-адреса реєстрації, дата та IP-адреса останнього відвідування тощо)..*

Слід зазначити, що за розповсюдження через соцмережі матеріалів із закликами до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України, передбачена кримінальна відповідальність.

3. Використання російських соціально-орієнтованих ресурсів мережі Інтернет

З 2016 року усі російські сервіси відповідно до федеральних законів РФ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» від 05.05.2014 року № 97-ФЗ, «О внесении изменений в Федеральный закон «О противодействии терроризму» від 06.07.2016 року № 374-ФЗ, «О внесении изменений в Уголовный кодекс РФ и Уголовно-процессуальный кодекс РФ в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» від 06.07.2016 року № 375-ФЗ та інших окремих законодавчих актів на постійній основі надають спецслужбам РФ відомості щодо персональних даних користувачів та їх особистого листування. Зважаючи на це, українські Інтернет-провайдери зобов'язані обмежити доступ користувачам до російських соціальних мереж та сервісів.

Крім того, слід пам'ятати, що доступ до російських соціальних мереж «ВКонтакте» та «Одноклассники» на території України заборонено рішенням Ради національної безпеки і оборони України від 14 травня 2020 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», введеного в дію Указом Президента України від 14.05.2020 року № 184/2020.

Головна порада – перехід на західні та українські сервіси, такі як «Gmail», «Facebook», «Twitter», «Ukr.net» тощо.

4. Використання додатків до смартфонів

Під час встановлення тих чи інших додатків на власний телефон ці програмні продукти можуть вимагати доступу до певної інформації на використовуваному пристрої, насамперед геолокації, списку контактів, акаунтів у соціальних мережах та поштових скриньок.

За наявними даними, більшість шпигунських програм «вшиваються» саме в мобільні додатки, які цікавлять конкретну аудиторію. Тому необхідно бути уважним під час встановлення

додатків, особливо якщо робити це з невідомих та неперевірених сервісів.

З метою унеможливлення завантаження на особистий пристрій програм-шпигунів необхідно дотримуватись таких правил:

- *встановлювати додатки лише з офіційних та перевірених сервісів (Chrome Store, Google Play Store для Android, App Store для iOS);*
- ***заборонити** операційній системі смартфона (планшета, ПЕОМ) автоматично встановлювати додатки з невідомих джерел, шляхом здійснення відповідних налаштувань пристрою;*
- *періодично здійснювати видалення усіх особистих пристроїв від додатків, які не використовуються.*

5. Електронне листування

Електронні поштові скриньки зберігають не тільки величезний обсяг особистих та робочих даних *(листів)*, але й зазвичай прикріплені до акаунтів у соціальних мережах, месенджерах, «хмарних» сервісах тощо. Враховуючи викладене, несанкціонований доступ до поштової скриньки може мати серйозні наслідки, такі як отримання інформації конфіденційного характеру, зміна паролів до сайтів, акаунтів без відома їх власників, отримання доступу до особистих фотографій та відео, розсилання спаму від імені інших осіб тощо.

Щоб уникнути зламу електронної поштової скриньки, необхідно:

- *увімкнути двофакторну автентифікацію за допомогою мобільного пристрою. В такому випадку під час спроби отримання паролю до поштової скриньки сторонніми особами буде надходити попередження на мобільний телефон у вигляді SMS-повідомлення про спробу злому;*
- *встановити надійний пароль;*
- ***не використовувати** для відновлення паролю російські сервіси («Yandex.ru», «Mail.ru» тощо);*
- ***не запускати** на пристроях вкладення підозрілих листів, що містять виконуваний файл з такими розширеннями як «.exe», «.bat», «.cmd», «.vbs», «.docm», «.xlsm» тощо;*
- *державні службовці повинні пам'ятати, що службові електронні скриньки не слід використовувати для приватного листування.*

6. Доступ до мережі Інтернет

Одним із найпоширеніших способів доступу до мережі Інтернет у публічних місцях є підключення до відкритих точок Wi-Fi. Зазвичай вони є безплатними та доступ до них здійснюється без введення паролів. Саме відсутність паролю робить їх вразливішими для злому з боку зацікавлених осіб, які мають на меті отримати персональні дані та відомості, що зберігаються на телефоні, планшеті, ПЕОМ тощо.

Щоб уникнути перехоплення даних сторонніми особами, необхідно:

- *під час здійснення доступу до мережі використовувати лише ті точки Wi-Fi, які мають протоколи безпеки для захисту безпровідного з'єднання WPA чи WPA-2;*
- *у публічних місцях найкраще користуватись особистим Wi-Fi модемом або здійснювати доступ до мережі Інтернет з мобільного пристрою за передплаченим пакетом послуг мобільного оператора;*
- *на ПЕОМ, мобільних пристроях та планшетах необхідно вимкнути функцію «Автоматичне підключення до Wi-Fi».*

7. Рекомендації посадовій особі органу виконавчої влади:

- *прес-службам державних органів під час суспільно-політичних подій в країні необхідно надавати коментарі та роз'яснення рішень на випередження, щоб уникнути інтерпретацій та викривлень у ході обговорення тієї чи іншої ситуації в загальнодоступних та соціально-орієнтованих ресурсах мережі Інтернет;*
- *державним органам, установам необхідно розробити та затвердити чіткий план дій для оприлюднення представниками їхніх прес-служб інформації у випадку виникнення резонансних інцидентів;*
- *офіційні представники органів державної влади повинні оприлюднювати суспільно значущу інформацію, якщо вона не належить до тієї категорії, що не підлягає оприлюдненню. Не варто забувати, що приховування такої інформації від суспільства може знизити довіру до них;*
- *представникам органів державної влади під час надання коментарів, інтерв'ю, брифінгів не рекомендується використовувати оціночні судження, що можуть призвести до неоднозначного тлумачення наданої інформації її споживачами;*
- *органам державної влади необхідно розробити правила використання офіційних сторінок та акаунтів у соціальних мережах для уникнення непорозумінь з користувачами та окреслення формату*

*комунікації через соціальні мережі. Крім того, вважається за доцільне здійснити верифікацію (довідково: **верифікація** – це офіційне підтвердження походження сторінки, її офіційного власника (фізичної, юридичної особи) автентичності викладеної інформації через службу технічної підтримки) офіційних представництв органів державної влади та установ, які у своїй діяльності використовують акаунти у соціальних мережах, насамперед «Facebook», «Twitter» та канали у відеохостингу «Youtube»;*

- *держслужбовцям, а також іншим особам, які відповідно до своїх функціональних обов'язків працюють з інформацією з обмеженим доступом, необхідно пам'ятати, що під час оформлення допуску до державної таємниці при заповненні відповідних анкет вони повинні вносити достовірні дані про свої контакти з іноземними громадянами, наявність власних електронних скриньок, сайтів, профілів у соціальних мережах та тематичних форумах.*

ВИТЯГ З КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ

Злочини проти основ національної безпеки України

Стаття 109. Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади

1. Дії, вчинені з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, а також змова про вчинення таких дій, -

караються позбавленням волі на строк від п'яти до десяти років з конфіскацією майна або без такої.

2. Публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій, -

караються обмеженням волі на строк до трьох років або позбавленням волі на той самий строк з конфіскацією майна або без такої.

3. Дії, передбачені частиною другою цієї статті, вчинені особою, яка є представником влади, або повторно, або організованою групою, або з використанням засобів масової інформації, -

караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк з конфіскацією майна або без такої.

Стаття 110. Посягання на територіальну цілісність і недоторканність України

1. Умисні дії, вчинені з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України,

а також публічні заклики чи розповсюдження матеріалів із закликами до вчинення таких дій, -

караються позбавленням волі на строк від трьох до п'яти років з конфіскацією майна або без такої.

2. Ті самі дії, якщо вони вчинені особою, яка є представником влади, або повторно, або за попередньою змовою групою осіб, або поєднані з розпалюванням національної чи релігійної ворожнечі, -

караються позбавленням волі на строк від п'яти до десяти років з конфіскацією майна або без такої.

3. Дії, передбачені частинами першою або другою цієї статті, які призвели до загибелі людей або інших тяжких наслідків, -

караються позбавленням волі на строк від десяти до п'ятнадцяти років або довічним позбавленням волі з конфіскацією майна або без такої.

Стаття 111. Державна зрада

1. Державна зрада, тобто діяння, умисно вчинене громадянином України на шкоду суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в умовах воєнного стану або в період збройного конфлікту, шпигунство, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України, -

карається позбавленням волі на строк від дванадцяти до п'ятнадцяти років з конфіскацією майна або без такої.

2. Звільняється від кримінальної відповідальності громадянин України, якщо він на виконання злочинного завдання іноземної держави, іноземної організації або їх представників ніяких дій не вчинив і добровільно заявив органам державної влади про свій зв'язок з ними та про отримане завдання.

Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, -

карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Стаття 361[-1]. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -

караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк до п'яти років.

Стаття 361[-2]. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, -

караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк від двох до п'яти років.

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, -

караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років.

2. Несанкціоновані перехоплення або копіювання інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, -

караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, -

караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Стаття 363[-1]. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -

карається штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, -

караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.