Тема 3. Цифрова безпека на персональному рівні

1. Публічна і персональна інформація: характеристика понять

2. Законодавство України про публічну інформацію та захист персональних даних. Стратегія формування цифрової грамотності серед населення України та цифрових компетентностей у професійній сфері

3. Найпоширеніші цифрові загрози, моделювання ризиків та основні кроки захисту персональних даних

4. Особливості документообігу та комунікації з точки зору цифрової безпеки в професійній діяльності

5. Безпекові правила роботи з організаційними соцмережами та сайтами

6. Кібератаки на громадянське суспільство та державний сектор – захист від фішингу

4. Особливості документообігу та комунікації з точки зору цифрової безпеки в професійній діяльності

Використання систем електронного документообігу (СЕД) дає змогу компанії отримати низку переваг, серед яких економія коштів, пришвидшення документообігу, виконання документів тощо. Водночас впровадження СЕД потребує здійснення певних заходів щодо забезпечення безпеки електронного обігу та зберігання документів.

Робота будь-якого суб'єкта господарювання чи установи так чи так пов'язана з рухом документів. Обсяг документообігу загалом залежить від того, на скільки велике підприємство, установа, організація і від напрямів його діяльності. Адже чим більше підприємство, тим більшу кількість документів генерує. Тому переведення їх у цифровий формат стає просто необхідним: **є суттєва різниця між створенням і зберіганням документа в паперовому й електронному форматі**.

Базовим елементом будь-якої СЕД є документ. Усередині системи це певний файл або відповідний запис у базі даних. Нагадаємо, що стаття 5 Закону України від 22 травня 2003 року № 851-IV «Про електронні документи та електронний документообіг» (*далі* — Закон про документообіг) містить таке визначення поняття електронного документа (ЕД):

Електронний документ - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Електронний підпис та електронна печатка

Для ідентифікації автора електронного документа може використовуватися електронний підпис.

Для підтвердження достовірності походження та цілісності електронного документа може використовуватися електронна печатка.

Накладанням електронного підпису та/або електронної печатки завершується створення електронного документа.

У разі створення електронного документа з використанням більш як одного електронного підпису та/або більш як однієї електронної печатки його створення завершується накладанням електронного підпису або електронної печатки останнім підписувачем чи створювачем електронної печатки відповідно до технології створення такого електронного документа.

Суб'єкти електронного документообігу використовують електронні підписи та електронні печатки у випадках, встановлених законодавством, або за домовленістю між відповідними суб'єктами.

Порядок використання електронного підпису у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю на яких здійснює Національний банк України, а також при наданні платіжних послуг визначається Національним банком України.

Порядок використання електронного підпису учасниками ринків капіталу та професійними учасниками організованих товарних ринків визначається Національною комісією з цінних паперів та фондового ринку.

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу.

Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії.

Електронна копія електронного документа засвідчується у порядку, встановленому законом.

Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством.

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Електронний документ не може бути застосовано як оригінал:

1) свідоцтва про право на спадщину;

2) документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;

3) в інших випадках, передбачених законом.

Нотаріальне посвідчення цивільно-правової угоди, укладеної шляхом створення електронного документа (електронних документів), здійснюється у порядку, встановленому законом.

Електронний документообіг (обіг електронних документів) - сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів.

Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством.

Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ.

Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, датою і часом відправлення електронного документа вважаються дата і час, коли відправлення електронного документа не може бути скасовано особою, яка його відправила. У разі відправлення електронного документа шляхом пересилання його на електронному носії, на якому записано цей документ, датою і часом відправлення вважаються дата і час здавання його для пересилання.

Вимоги підтвердження факту одержання документа, встановлені законодавством у випадках відправлення документів рекомендованим листом або передавання їх під розписку, не поширюються на електронні документи. У таких випадках підтвердження факту одержання електронних документів здійснюється згідно з вимогами цього Закону.

Одержання електронних документів

Електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб’єктами електронного документообігу.

Якщо попередньою домовленістю між суб’єктами електронного документообігу не визначено порядок підтвердження факту одержання електронного документа, таке підтвердження може бути здійснено в будь-якому порядку автоматизованим чи іншим способом в електронній формі або у формі документа на папері. Зазначене підтвердження повинно містити дані про факт і час одержання електронного документа та про відправника цього підтвердження.

У разі ненадходження до автора підтвердження про факт одержання цього електронного документа вважається, що електронний документ не одержано адресатом.

Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, електронний документ вважається відправленим автором та одержаним адресатом за їх місцезнаходженням (для фізичних осіб - місцем проживання), у тому числі якщо інформаційна, електронна комунікаційна, інформаційно-комунікаційна система, за допомогою якої одержано документ, знаходиться в

іншому місці. Місцезнаходження (місце проживання) сторін визначається відповідно до законодавства.

Перевірка цілісності електронного документа проводиться шляхом підтвердження удосконаленого або кваліфікованого електронного підпису чи печатки, а в разі накладання на електронний документ електронного підпису чи печатки іншого виду - із застосуванням інших засобів і методів захисту інформації з дотриманням вимог законодавства у сфері захисту інформації.

Зберігання електронних документів та архіви електронних документів

Суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

У разі неможливості зберігання електронних документів на електронних носіях інформації протягом строку, встановленого законодавством для відповідних документів на папері, суб'єкти електронного документообігу повинні вживати заходів щодо дублювання документів на кількох електронних носіях інформації та здійснювати їх періодичне копіювання відповідно до порядку обліку та копіювання документів, встановленого законодавством. Якщо неможливо виконати зазначені вимоги, електронні документи повинні зберігатися у вигляді копії документа на папері (у разі відсутності оригіналу цього документа на папері). При копіюванні електронного документа з електронного носія інформації обов'язково здійснюється перевірка цілісності даних на цьому носії.

При зберіганні електронних документів обов'язкове додержання таких вимог:

1) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

2) має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;

3) у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Суб'єкти електронного документообігу можуть забезпечувати додержання вимог щодо збереження електронних документів з накладеними на них електронними підписами чи печатками шляхом використання електронної довірчої послуги зберігання електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, відповідно до Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

Створення архівів електронних документів, подання електронних документів до архівних установ України та їх зберігання в таких установах здійснюються у порядку, визначеному законодавством.

Організація електронного документообігу

Електронний документообіг здійснюється відповідно до законодавства України або на підставі договорів, що визначають взаємовідносини суб'єктів електронного документообігу.

Використання електронного документа у цивільних відносинах здійснюється згідно із загальними вимогами вчинення правочинів, встановлених цивільним законодавством.

Електронний документообіг на платіжному ринку здійснюється з урахуванням Закону України "Про платіжні послуги".

Обіг електронних документів, що містять інформацію з обмеженим доступом

Суб'єкти електронного документообігу, які здійснюють його на договірних засадах, самостійно визначають режим доступу до електронних документів, що містять конфіденційну інформацію, та встановлюють для них систему (способи) захисту.

В інформаційних, електронних комунікаційних, інформаційно-комунікаційних системах, які забезпечують обмін електронними документами, що містять державні інформаційні ресурси, або інформацію з обмеженим доступом, повинен забезпечуватися захист цієї інформації відповідно до законодавства.

Захист інформації під час виконання платіжних операцій здійснюється з урахуванням вимог Закону України "Про платіжні послуги".

Права та обов'язки суб'єктів електронного документообігу

Суб'єкти електронного документообігу користуються правами та мають обов'язки, які встановлено для них законодавством.

Якщо в процесі організації електронного документообігу виникає необхідність у визначенні додаткових прав та обов'язків суб'єктів електронного документообігу, що не визначені законодавством, такі права та обов'язки можуть встановлюватися цими суб'єктами на договірних засадах.

Вирішення спорів між суб'єктами електронного документообігу здійснюється в порядку, встановленому законом.

Особи, винні в порушенні законодавства про електронні документи та електронний документообіг, несуть відповідальність згідно з законами України.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

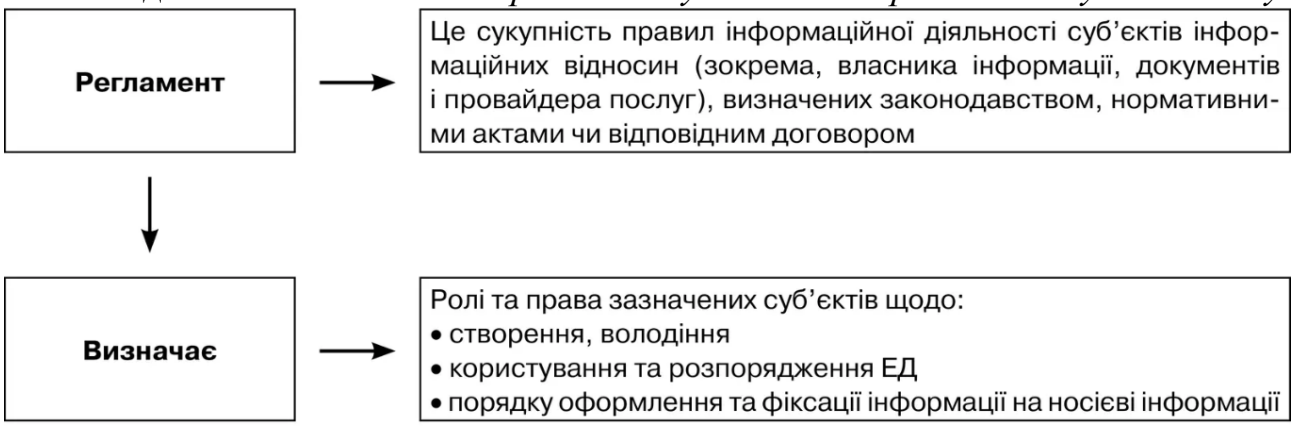
Обов'язковими реквізитами ЕД є дані, без яких він не може бути підставою для його обліку і не матиме юридичної сили. Відповідно до ст. 6 Закону про документообіг, **для ідентифікації автора електронного документа** може використовуватися **електронний підпис**. Накладанням електронного цифрового підпису (ЕЦП) завершується створення ЕД.

Тільки ЕЦП за правовим статусом прирівнюється до власноручного підпису, тоді як інші види електронного підпису такого статусу не мають.

Сервіси електронного документообігу надаються відповідно до Закону України від 05 жовтня 2017 року № 2155-VIII «Про електронні довірчі послуги» (*далі* — Закон № 2155). Ним врегульовані відносини, що виникають між юридичними, фізичними особами, суб'єктами владних повноважень у процесі надання, отримання електронних довірчих послуг, процедури надання цих послуг, нагляду (контролю) за додержанням вимог законодавства у сфері електронних довірчих послуг, а також основні організаційно-правові основи електронної ідентифікації.

Варто зазначити, що **електронна довірча послуга** — це послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги. Вибираючи надавача таких електронних довірчих послуг — провайдера електронного документообігу, необхідно звертати на низку факторів, які повинні забезпечити повноцінну і захищену роботу з даними підприємства-замовника.

Надзвичайно важливим є *регламентування електронного документообігу*.



ЗАГРОЗИ ДЛЯ СЕД

Практика показує, що нині є чимало підприємств, котрі, впроваджуючи СЕД, висловлюють побоювання щодо випадкового чи навмисного знищення (втрати) ЕД. Однак якщо говорити про паперові версії документів, то на 100 % захистити їх від крадіжок, втрати, випадкового чи умисного знищення практично неможливо. Водночас електронний формат документів — це **спосіб захистити дані кількома рівнями**.

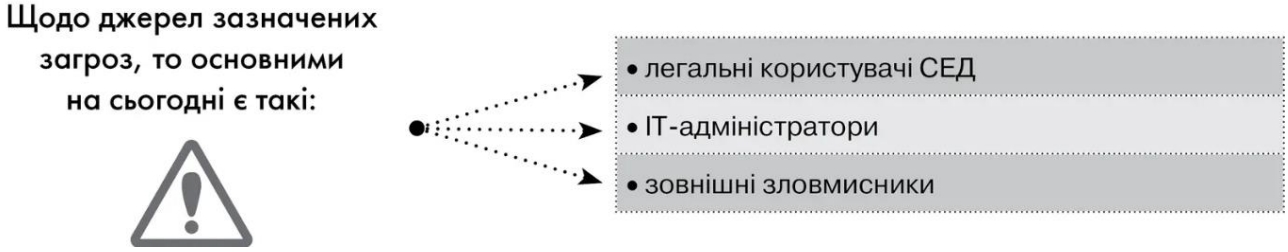
Але спочатку пропонуємо розглянути, які загрози існують сьогодні для ЕДО. Однією з найважливіших вимог до будь-якої СЕД є забезпечення безпеки електронного обміну документами. Згідно з Законом України від 05 липня 1994 року № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах», **захист інформації** — діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі. При цьому **відповідальність за забезпечення захисту інформації покладається на власника системи**.

1 Загроза цілісності інформації — пошкодження, знищення або перекручення інформації, як не навмисне (в разі помилок і збоїв), так і зловмисне

2 Загроза конфіденційності — будь-яке порушення конфіденційності, зокрема крадіжка, перехоплення інформації, зміна маршрутів доставки тощо

3 Загроза роботі системи — загрози, реалізація яких може призвести до порушення або припинення роботи СЕД (умисні атаки, помилки користувачів, збої в устаткуванні і програмному забезпеченні).

4 Загроза доступності — здійснення дій, які унеможливлюють чи ускладнюють доступ до СЕД, зокрема, створення таких умов, при яких доступ до послуги чи інформації або заблокований, або можливий за час, який не забезпечить виконання тих чи інших цілей.



Користувач СЕД є потенційним внутрішнім зловмисником, який може нашкодити свідомо чи з необережності. Водночас спектр можливих загроз від **легальних користувачів** доволі широкий, починаючи від банальних скріпок, поміщених в апаратну частину системи до навмисних крадіжок з корисливою метою чи пошкодження носіїв з помсти.

Персонал IT-служби підприємства є особливою групою ризику, до якої слід поставитися з особливою увагою. Зазвичай ці спеціалісти мають широкі, а нерідко і практично необмежені повноваження і доступ до сховищ даних. До того ж вони найбільш кваліфіковані в питаннях безпеки та інформаційних можливостей. Як свідчать численні дослідження, майже 80 % втрат документів та інформації пов’язані з діями «внутрішнього ворога».

Щодо **зовнішніх зловмисників**, то тут все залежатиме від сфери діяльності підприємства, організаційної форми, наявності конкурентів тощо. Тобто причиною атак можуть слугувати здебільшого міжособистісні конфлікти між власниками підприємства і партнерами, конкурентами, незадоволеними клієнтами.

СПОСОБИ ЗАХИСТУ СЕД

Безпосередній захист СЕД на підприємстві можна організувати різними способами. Як уже зазначалося, багато власників інформації та документів все ще побоюються вводити електронний документообіг саме з причин безпеки, втрачаючи при цьому час і кошти. Але нині ринок цих послуг в Україні доволі розвинений, тому кожен може вибрати собі провайдера з огляду на власні потреби й фінансові можливості. Та якщо власникові чи керівникові не байдужі питання безпеки (а так має бути), варто звернути увагу на показники, які пропонує постачальник послуг.

Зрозуміти, що СЕД надійна, можна за кількома показниками:

1. **Забезпечення збереження ЕД.** Насамперед це резервне копіювання ЕД. Також сюди входить зберігання ЕД в архіві, який знаходиться в захищеному хмарному середовищі на декількох дата-центрах.
2. **Закритий доступ до СЕД.** Щоб увійти всвій акаунт, користувач СЕД має пройти аутентифікацію. Це може бути **один спосіб**, наприклад, *пароль, USB-ключ* чи *відбиток пальця*. А може бути і **багатоетапний**, що містить кілька кроків: *пароль і ключ* або *пароль і біометрична фіксація*. Максимально надійний для проведення ідентифікації й подальшої аутентифікації спосіб —

біометричний, за якого користувач ідентифікується за своїми біометричними даними (відбиток пальця, сканування сітківки ока, голос). Однак у цьому випадку вартість СЕД є вищою незважаючи на те, що сучасні біометричні технології ще не настільки досконалі, щоб уникнути помилкових спрацьовувань або відмов. До того ж техніка користувачів має відповідати вимогам біометричної фіксації даних.

3. **Розмежування прав доступу.** Цей функціонал дає змогу мати доступ до окремих документів лише певному колу користувачів. Інші користувачі, відповідно, такого права позбавлені. Також він може передбачати не лише можливість доступу до документів, а й дозвіл на їх підписання за допомогою ЕЦП.

4. **Ступінь конфіденційності.** Для дотримання конфіденційності в СЕД можуть застосовуватися криптографічні методи шифрування даних, які ніхто, крім їх власника і призначених ним користувачів, не зможе бачити. Застосування криптографії не дадуть шансу порушити конфіденційність ЕД навіть у разі його потрапляння до сторонніх осіб.

5. **Забезпечення достовірності інформації.** Поки що основним і практично єдиним із запропонованих на ринку рішенням для забезпечення достовірності документа є ЕЦП. Зрозуміти, що документ чинний можна за наявності ЕЦП. Зокрема, відповідно до ст. 7 Закону про документообіг, оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону № 2155. Більшість виробників СЕД вже мають вбудовані у свої системи, власноруч розроблені або партнерські засоби для використання ЕЦП.

6. **Протоколювання дій користувачів СЕД.** Це один із важливих елементів захисту електронного документообігу. За умови його правильного налаштування та реалізації в СЕД протоколювання дає можливість відстежувати всі неправомірні дії користувачів та знаходити «винуватця», а в разі оперативного втручання — навіть зупинити спробу неправомірних або шкідливих дій.

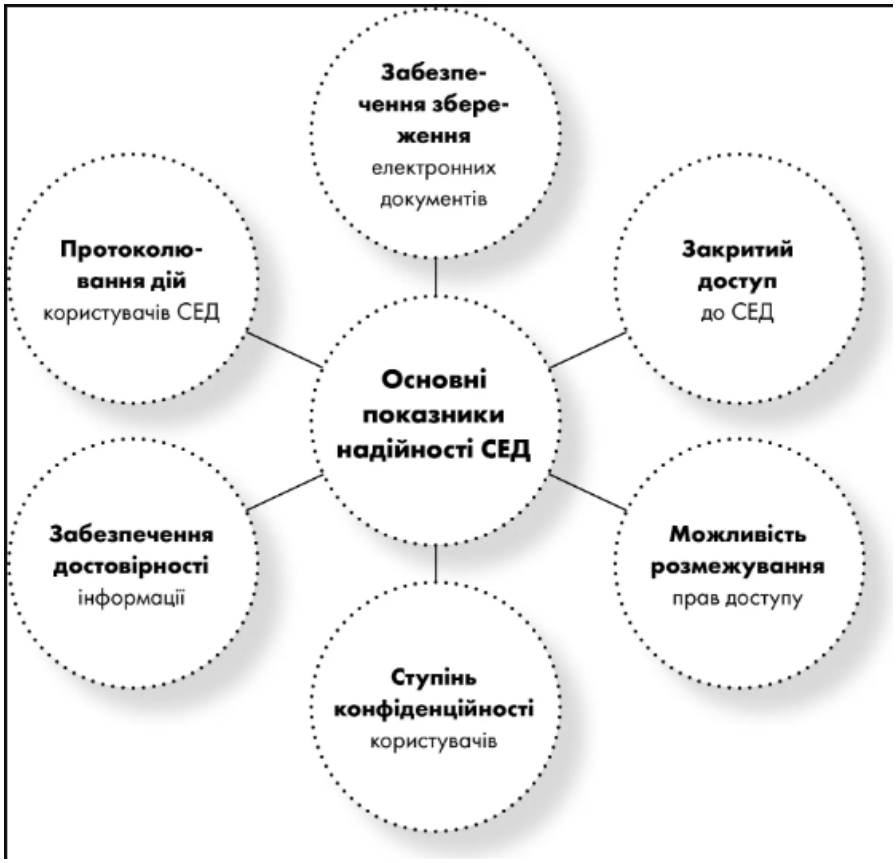


Рис. 1. Деякі критерії надійності СЕД

ОРГАНІЗАЦІЯ І ЛОЯЛЬНІСТЬ

Крім технічних, не варто забувати і про організаційні заходи захисту. Якою б ефективною не була система захисту СЕД та криптографія, мало що може завадити третій особі прочитати документ, наприклад, стоячи за спиною користувача, який має до нього доступ на законних підставах. Не виключається, що зловмисник зможе розшифрувати інформацію з ЕД, скориставшись ключем, який залишений працівником у відкритому доступі, наприклад, на робочому столі під час його відсутності.

Основне проблемне місце в організації захисту СЕД — це не стільки технічні засоби, як *лояльність* її користувачів. Слід розуміти, що коли документ потрапляє до користувача, його конфіденційність вже порушена. Якщо цей користувач має злі наміри, запобігти витоку документа через нього суто технічними заходами практично неможливо. Він може знайти безліч способів скопіювати інформацію, від збереження його на зовнішній носій до банального фотографування. Саме тому тут на допомогу приходить зазначене вище *протоколювання дій користувачів*.

Як бачимо, **підхід до захисту електронного документообігу має бути комплексним**. Необхідно чітко розуміти і об'єктивно оцінювати можливі загрози та ризики для СЕД і величину можливих втрат. Захист СЕД не зводиться лише до захисту документів і розмежування доступу до них. Важливими є питання захисту:

- апаратних засобів системи, персональних комп'ютерів, принтерів та інших пристроїв;
- мережевого середовища, в якому функціонує система;
- каналів передавання даних і мережевого устаткування;

Крім цього, перевагою є можливе виділення СЕД в особливий сегмент мережі. Тому під час вибору засобів захисту СЕД необхідно **оцінити** реальні втрати від розголошення або спотворення інформації і **співставити** їх із вартістю засобів, які мають бути впроваджені для їх охорони. В будь-якому разі мають бути застосовані хоча й елементарні та не надто дорогі, але не менш ефективні засоби, наприклад, вхід до СЕД повинен здійснюватися *за системою паролів з розмежованим рівнем доступу*. Фізичний доступ у приміщення, де встановлена система керування документообігом, повинен здійснюватися за правилами внутрішнього розпорядку і бути обмеженим для сторонніх осіб.

Отже, рівень комплексу організаційних заходів відіграє важливу роль на кожному етапі захисту. Недбалість та неналежна організація може звести нанівець усі технічні заходи, незважаючи на їх досконалість та високу вартість.

5. Безпекові правила роботи з організаційними соцмережами та сайтами

Зазвичай ми розділяємо соцмережі організацій на два типи: із доступом через особисті акаунти та через окремі акаунти, адже безпекова робота над ними в такому разі різна.

Соцмережі з доступом через особисті акаунти потребують захисту власне цих особистих акаунтів, а не лише самої сторінки. За таким принципом працюють Facebook-сторінки і Telegram-канали.

Коли організація створює Facebook-сторінку, то людина, яка її створила, автоматично стає адміністратором сторінки. Далі ця людина запрошує інших користувачів та може надавати їм різні права доступу.

Які вони можуть бути:

Адміністратор – має найбільше прав на сторінці, може її видаляти, додавати та забирати права доступу в інших користувачів.

Редактор – може додавати та видаляти контент на сторінці.

Модератор – може коментувати від імені сторінки.

Схожа ситуація при створенні Telegram-каналу. Людина, яка створила Telegram-канал, автоматично стає власником та адміністратором каналу.

У роботі з цими соцмережами насамперед потрібно звертати увагу на те, хто які доступи має до сторінки. Тут стане у пригоді документ із активами організації. Інформацію про те, хто має доступи, хто адміністратор тощо, можна також додавати в нього.

На що потрібно звертати увагу, працюючи з такими соцмережами?

Визначте людину, відповідальну за акаунт.

Контроль доступів – складний процес. Без відповідальної людини контролювати доступи складно, а сам процес стає хаотичним. В ідеалі потрібно визначити, хто в команді контролює доступи до соцмереж чи до певних сторінок. Це може бути комунікаційник або смм-ник, наприклад.

Хто має доступ?

Найкраще, коли доступ до сторінок мають лише люди, які з ними працюють. Якщо людина перейшла на іншу позицію і вже не працює з соцмережами або не працює в команді, потрібно забрати в неї доступ до сторінки, адже це створює додаткові ризики для організації. Наприклад, під час інцидентів важче зрозуміти, через кого зламали сторінку.

Кому належить власність?

Разом із тим права власності сторінки/каналу повинен мати хтось із керівництва організації або засновники – навіть якщо вони не займаються соцмережами, адже власники мають найбільше прав.

Хто адміністратор?

Адміністраторами також не мають бути всі – такі права потрібно надавати керівнику чи керівниці комунікаційного відділу або людині, яка найбільше працює зі сторінкою. Крім того, на випадок недоступності адміністратора, варто додати резервного адміністратора. Ним може бути керівник організації.

Захист акаунтів

Наступний крок – це захист особистих облікових записів. Розпочати треба з адміністраторів, адже якщо зламають їхні облікові записи, то отримають найбільше прав доступу до організаційних сторінок чи каналів та зможуть видалити решту користувачів або саму сторінку.

На які пункти варто звертати увагу при захисті акаунта?

Двофакторна автентифікація. У Telegram (і в месенджерах загалом) є нюанс: першим фактором є код із смс, а другим – пароль. Щоб уникнути випадків втрати цього пароля, потрібно додати резервну пошту. Ця пошта також має бути захищеною.

Контактні дані. Акаунт має бути зареєстровано на актуальну та захищену пошту. У Facebook є нюанс: якщо ви змінювали пошту – стара не зникає, а стає резервною, тому звертайте на це увагу.

Сповіщення про вхід у Facebook. При вході з нового місця/пристрою приходитиме сповіщення у Facebook та на пошту

Наприклад, Twitter чи Instagram, коли для того, аби надати доступ, ми ділимося паролем та логіном для входу. Із ними виникає багато труднощів із погляду безпеки, адже переважно доступ до акаунта повинні мати кілька людей. Як безпечно ділитися логіном та паролем між собою? Як зрозуміти, хто зайшов в акаунт? Як ділитись двофакторною автентифікацією?

Правильних відповідей тут немає, адже тут ми як ніколи бачимо, що безпека – це компроміс між власне безпекою та комфортом. Якщо цей процес буде складним та незручним для всіх, навіть якщо він ідеальний для захисту від зловмисників – це все одно призведе до того, що працівники шукатимуть способів обійти ці функції.

Визначте людину, відповідальну за акаунти.

Коли є хтось відповідальний за цифрові активи, контролювати доступи та

безпеку стає значно простіше. Ця людина може надавати та забирати доступи, стежити за сповіщеннями безпеки, передавати паролі тощо.

Поширення паролів.

Насамперед подумайте про кілька варіантів та тестуйте їх. Якщо ви обрали якийсь спосіб і він вам не підходить, ви цілком можете його змінити та пробувати інші. Наприклад, паролі можна поширювати через парольні менеджери. Але для цього має бути один парольний сервіс, яким користується організація.

Досить часто організації використовують пошту або ж месенджери для передачі паролів, навіть якщо вважають цей спосіб не дуже безпечним. Що робити в такому разі? Ділитися паролями таким чином можна, але варто зважати на безпеку також. Наприклад, можна обрати якийсь месенджер, передати паролі працівникові, і після того, як він їх збереже - видалити їх із чату. Наприклад, у месенджерах є функція видалення «для всіх» навіть після прочитання повідомлення.

Двофакторна автентифікація.

Виберіть варіант, який вам найкраще підходить. Про способи двофакторної автентифікації, є: смс, генератор кодів, резервні коди та фізичний ключ. Наприклад, налаштуйте двофакторну автентифікацію на людину, відповідальну за акаунт. Тоді ця людина передаватиме коди колегам при новому вході та контролюватиме нові входи. Інший спосіб – налаштувати генератор кодів на телефонах кількох людей. Тоді кожен зможе самостійно входити в акаунти, маючи пароль та другий фактор, і не залежати від зв’язку з однією визначеною людиною. Головне при цьому всьому – мати резервні способи двофакторної автентифікації та змінити її спосіб після звільнення працівника, який мав до неї доступ. Наприклад, якщо комусь приходили коди з смс, а ця людина звільнилася – змінити номер телефону. Резервні способи рекомендуємо зберігати в керівництва організації, щоб запобігти їхній втраті.

Активні сесії.

Тепер перейдемо до спільних активних сесій. Ситуація: кілька працівників мають доступ до організаційного Instagram і заходять туди з кількох особистих пристроїв. Як тоді зрозуміти – це колега зайшов чи хтось інший? Рекомендуємо такий спосіб:

- насамперед, як ми говорили раніше, потрібно обрати одну людину, відповідальну за акаунт;
- далі можете обрати певний період, наприклад, місяць чи три місяці, і закривати всі активні сесії в акаунті;
- коли людина, відповідальна за акаунт, бачить новий вхід – перепитувати працівників, хто саме ввійшов в акаунт

Отже, для захисту соцмереж нам потрібно звертати увагу на доступи та захист акаунтів, а також обрати людину, яка відповідатиме за це.

Чимало організацій мають свої сайти, де збирають та публікують інформацію про свою діяльність або про теми, з якими працюють. Вебсайт – це

набір програм, файлів та баз даних, що зберігаються в хостинг провайдера. Коли організація хоче розробити сайт, вона звертається до веб-розробників, реєструє доменне ім'я – назву сайту, знаходить хостинг-провайдера. Тож сайт – це доволі складний продукт, що вимагає постійних витрат ресурсів.

Якщо у вашій організації є важливі сайти, то пропонуємо список для самоперевірки, щоб краще зрозуміти захищеність вашого веб-сайту від зламу чи втрати.

Відповідальний за сайт

Переважно такі речі, як сайти, соцмережі, доступи до документів не входять у перелік обов'язків працівників, особливо якщо в організації немає IT-спеціаліста. Тож завжди важливо мати людину в організації, відповідальну за технічні процеси й доступи. До сайту входить також оплата за хостинг та доменне ім'я, адже це напряму пов'язано з доступністю сайтів.

Домен

Перш ніж запустити сайт, організації потрібно придумати назву домену та придбати її в доменного реєстратора. За домен потрібно регулярно сплачувати, щоб він продовжував працювати. Тут важливі декілька моментів:

- на кого в організації зареєстрований домен? Ідеальний варіант, коли домен зареєстрований на юридичну особу
- хто має доступ до панелі керування доменом? Цей доступ може знадобитися в разі перенесення сайту на новий хостинг, додавання нових імен тощо. Резервна копія такого доступу повинна зберігатися в керівництва організації.
- хто і як часто оплачує послугу оренди домену? Нерідко трапляються випадки, коли за несплату за домен, він перестає працювати або ж його викуповують брокери й потім вимагають значно більше коштів за його повернення першим власникам.

Хостинг та сервери

Через блекаути можуть виникати проблеми з доступом до сайту, якщо сервери вашого хостера розміщені на території України і він не забезпечив резервного живлення. Тому варто уточнити у провайдера хостингу, наскільки він підготовлений до блекаутів, особливо довгих, а також чи робить він резервні копії вашого сайту та баз даних. Так само як у випадку з доменом, звертаємо увагу на такі моменти:

- на кого зареєстрований акаунт адміністратора панелі управління хостингом;
- хто ще має доступ до цієї панелі;
- хто і як часто оплачує послуги хостингу

Резервні копії

Сайт та його контент можна втратити. Якщо ваш сайт відіграє роль інформаційного архіву й потрібно будь-що зберегти всю опубліковану інформацію – вам потрібні офлайнові резервні копії. Таке резервне копіювання

може налаштувати веб-адміністратор. Важливо, щоб ці копії були доступні керівництву організації в будь-який момент. Частота резервного копіювання залежить від інтенсивності наповнення сайту новою інформацією.

Захист від DDoS-атак

Якщо вам важлива постійна доступність вашого сайту, рекомендуємо подбати про захист від DDoS. Такий захист також може налаштувати веб-адміністратор. Є безліч сервісів, що пропонують такий захист. Один із них – Cloudflare. Він має як платні, так і безкоштовні опції.

Захист від зламу

Щоб убезпечити сайт від зламу, треба розпочати з аудиту доступів. Доступи з правами адміністратора повинні мати люди, які вносять суттєві зміни на сайт та контролюють доступи іншим. Тим, хто публікує контент, цілком можна мати доступи редакторів. Окрім цього, акаунти мають бути захищеними надійними паролями – довгими та унікальними.

Оновлення

Сайт може бути скомпрометований через застарілі плагіни чи код. Тому не забувайте регулярно оновлювати сайт і плагіни.

Підтримка

Робота з сайтами вимагає специфічних технічних кваліфікацій. Якщо для вас важлива доступність та захищеність вашого сайту, рекомендуємо долучати технічних спеціалістів або компанії для обслуговування сайту. При виникненні проблем із сайтом технічна підтримка допоможе швидко їх вирішити.

Тепер ви знаєте на що потрібно звертати увагу, щоб соцмережі та сайти вашої організації були безпечнішими.

Ще одне поширене запитання щодо безпеки – а де взагалі спілкуватися з командою? Який спосіб найбезпечніший? Почнемо з другого: нам не завжди потрібен найбезпечніший спосіб. Потрібен той, що відповідає саме вашим потребам та ризикам, і просто добре захищений, а вибір самої платформи не вирішить усіх проблем безпеки, навіть якщо це найбезпечніший месенджер.

Перед тим, як перейти до вибору платформи для спілкування, насамперед визначаємо свої потреби – це обмін робочими файлами, організаційні чати про те, хто коли приходить в офіс, обговорення поточних завдань тощо. Цілком легітимно обрати кілька варіантів залежно від потреб організації. Наприклад, месенджер – для швидкої комунікації в команді, Slack для комунікації щодо проєктів та поточних завдань, а Trello чи Asana для постановки завдань. Цілком легітимно змінювати платформи, тестувати та обирати ті, що підходять саме вашій організації.

Наступне, на що ми звертаємо увагу – це наскільки чутливою інформацією ви обмінюєтеся з колегами. Наприклад, якщо це переписки з конфіденційною інформацією, розголошення якої матиме серйозні наслідки для організації чи інших людей, використовуйте месенджери з шифруванням із кінця в кінець. Серед популярних це Signal та WhatsApp.

Для чатів із конфіденційною інформацією корисна функція автовидалення – переписка автоматично видалятиметься через обраний період (від доби до кількох місяців). Якщо пристрій одного з учасників чату буде скомпрометовано, зловмисники отримають доступ лише до частини переписки, а не до всього архіву повідомлень. Але варто пам'ятати, що переписки, які були в чатах до ввімкнення цієї функції, не видалятимуться, тому її потрібно видаляти вручну.

Якщо ви користуєтеся чатами для обговорення поточних завдань і спілкування з колегами та не вбачаєте серйозних наслідків у разі якщо хтось отримає до них доступ – ви можете використовувати зручні вам платформи.

І найголовніше – який би сервіс ви не обрали, важливо подбати про захист акаунтів від зламу. Наприклад, якщо ви користуєтесь Signal, бо це «найбезпечніший» месенджер, але не налаштували двофакторну автентифікацію, то ваші чати будуть вразливими до віддалених атак. Звісно, там є шифрування і зловмисник не побачить попередні переписки, але він зможе побачити наступні та імперсонізувати вас. Особливо важливо налаштувати захист акаунтів адміністраторів групових чатів, адже вони можуть додавати чи забирати доступи, видаляти чати тощо. Також має бути відповідальна людина, яка контролює доступи до чату.

Ви можете створювати кілька чатів чи груп для зручнішого спілкування, ефективної роботи та безпеки. Наприклад, у чаті, де обговорюються різні заявки для донорів тощо, не повинні бути всі працівники, а тільки ті, які беруть участь у роботі над заявкою. А в чаті для комунікаційників не мають бути всі працівники, а ті, хто займається комунікаціями.

Отже, обираючи сервіси для внутрішньої комунікації потрібно враховувати потреби та вміст переписок, крім цього важливо подбати про захист акаунтів та контроль доступів.

6. Кібератаки на громадянське суспільство та державний сектор – захист від фішингу

За різними даними, понад сто країн здатні здійснювати спонсоровані державою кібератаки. Конфлікт між росією та Україною служить прикладом того, як дві сильні кібердержави можуть використовувати свої ресурси для досягнення цілей своїх країн, постійно діючи одна проти одної. Ця війна пролила світло на восьмирічний кіберконфлікт, який минулого року вилився в кінетичні елементи. З огляду на те, що міжнародні протистояння дедалі частіше відбуваються в сірій зоні між миром і війною, багато національних урядів мають використовувати кіберзахист України як інструмент для навчання. Реорганізація з метою посилення можливостей у кіберпросторі та кращого захисту від кіберзагроз була головним пріоритетом для багатьох країн ще до цього конфлікту. Хоча дві третини всіх країн вже запровадили політику захисту від небезпек у кіберпросторі, потрібні більш масштабні заходи. Величезна кількість країн, здатних проводити наступальні кібероперації, та ефективність оборони України, підкреслюють необхідність правильних структур і зв'язків для

комплексної та успішної боротьби з кіберзахистом. Ця кібербитва примітна тим, як Україна здійснила потужний кіберзахист від кібердержави вищого рівня за допомогою національних урядів, громадськості та бізнес-сектору.

Є кілька важливих уроків, які інші уряди повинні винести з попереднього року, протистоячи кібератакам з інших джерел, окрім Росії, навіть якщо важко узагальнити уроки кіберзахисту України.

Значення кіберзахисту в російсько-українській війні

До вторгнення Росії в Україну ніколи не було кінетичної битви між двома надзвичайно потужними кібердержавами. На відміну від нищівних втрат, які Росія завдає Україні, вона змогла ефективно захистити свої інтереси, підкреслюючи важливість кіберпотенціалу в звичайних бойових діях. Протягом багатьох років Україну закликали зміцнити свій кіберзахист і запровадити кіберзахист "усього суспільства". Особлива обстановка цієї війни, яка включає триваючий конфлікт сірої зони та безпрецедентні ресурси від міжнародних гравців і приватного сектору, ускладнює узагальнення уроків, отриманих з неї. Однак національні уряди, які прагнуть зміцнити свої власні в майбутньому, повинні розглянути кіберзахист України станом на сьогоднішній день.

Професійні кіберзахисники

Незважаючи на те, що Росія вторглася в Україну 24 лютого 2022 року, з моменту незаконного захоплення Криму в 2014 році, Україна захищається від російських кібератак. Атаки також посилилися перед вторгненням. Російські напади на державний, енергетичний, медійний, фінансовий, комерційний та благодійний сектори України відбувалися часто протягом останніх десяти років. У 2015 році Росія відключила частину енергомережі України, в результаті чого 230000 людей залишалися без світла протягом шести годин. ГРУ ГШ РФ використала вірус NotPetya у 2017 році для атаки на сотні підприємств і лікарень по всьому світу, включно з енергетичною інфраструктурою України. З початку кінетичного протистояння Росія використовувала свої кіберпотужності, щоб робити все: від блокування доступу до основних послуг до крадіжки даних, дезінформації, зловмисного програмного забезпечення, DDoS-атак, фішингових електронних листів і програмного забезпечення для спостереження. Незважаючи на ці перешкоди, Україна змогла скоординувати свої таланти, ресурси та зв'язки, щоб блокувати та відновлювати невдачі за невдачами в кіберпросторі. Інвестиції як у фінансові, так і в людські ресурси, щоб гарантувати набір і утримання кваліфікованих спеціалістів з кібербезпеки, є критично важливою частиною кіберзахисту. Важко ігнорувати, наскільки зрілими є українські операції безпеки та реагування на інциденти, а також перевірені в боях кіберзахисники.

Цілісний національний план кібербезпеки

Понад дві третини країн сьогодні вже мають план кібербезпеки, щоб керувати своїм повним кіберзахистом. Затвердження Національної стратегії кібербезпеки України на 2016 рік, у якій визнається значущість усіх гравців у зміцненні кіберзахисту України, як в уряді, так і поза ним, стало важливою віхою в консолідації національних кіберспроможностей країни. Запровадження законів і нормативних актів щодо кіберзлочинності та кібербезпеки, впровадження технічних заходів для забезпечення наявності досвіду для підвищення кіберстійкості, встановлення організаційних заходів для забезпечення координації між урядовими установами та відповідними суб'єктами, а також

розвиток потенціалу через зростання вітчизняних галузей кібербезпеки, інвестиції в програми досліджень і розробок і забезпечення фінансування досліджень і розробок – це лише кілька способів, якими національні уряди можуть підвищити свою кіберстійкість. Щоб зміцнити комплексну кібербезпеку України, український уряд працював над посиленням співпраці між усіма державними організаціями, органами місцевого самоврядування, військовими частинами, правоохоронними органами, дослідницькими організаціями та громадянським суспільством.

Найкращі плани кіберзахисту включають військові операції та збір інформації в більші національні цілі. Крім того, щоб не відставати від мінливих загроз і підвищувати національну стійкість, кіберплани необхідно регулярно оновлювати та змінювати. Стратегія України після вторгнення Росії у 2022 році, зазнала суттєвих змін, які охопили ширше коло учасників, зокрема, суб'єктів господарювання, громадських об'єднань та окремих громадян України для вирішення проблеми кібербезпеки країни.

Урядовий централізований кіберзахист

Національні уряди все більше консолідують численні відділи, відповідальні за різні аспекти кібероперацій. Такі структури, як розвідувальні агентства, військові, правоохоронні органи та дипломатична служба, усі мають окремі функції в уряді; але для кіберзахисту ці часто незалежні частини повинні співпрацювати. Національний координаційний центр з кібербезпеки (НЦКК) був створений в результаті реалізації кіберполітики Уряду України в 2016 році. НЦКК здійснює нагляд та оцінку стану національної кібербезпеки, включаючи підготовку до протидії кібератакам, а також виявлення та прогнозування можливих і поточних загроз. НКЦК об'єднує частини Ради національної безпеки і оборони України. Крім того, НКЦК пропонує міжвідомчі та міжнародні навчальні програми. Ефективна організація та координація федерального кіберзахисту України показує, як ці інструменти мають бездоганно інтегруватися для досягнення оптимальної ефективності.

Союзники обмінюються технологіями та розвідними даними до та під час конфлікту

Міжнародна допомога, яку Україна отримала і досі отримує, є однією з особливостей кіберзахисту, що змінює правила гри. Цю допомогу надали такі країни, як США та Великобританія, а також міжнародні організації, такі як ЄС і НАТО, у формі кіберекспертизи та розвідки.

Задовго до лютневого вторгнення Україна отримувала підтримку та співпрацю від міжнародної кіберспільноти. З 2014 року іноземні союзники мобілізували ресурси для зміцнення кіберзахисту України, одночасно зміцнюючи свій власний, зокрема ЄС, США та Великобританія. Перша двостороння кіберрозмова між США та Україною відбулася в 2017 році, і учасники поділилися методами створення організацій з кібербезпеки та протоколами реагування на кіберінциденти. Відтоді США допомогли Україні розширити її кіберспроможність на суму 40 млн. дол.. Щоб підвищити стійкість кібербезпеки України та підвищити її регулювання, ЄС розпочав з нею кіберрозмову у 2021 році. Кіберпрофесіонали з Кіберкомандування США та Українського кіберкомандування співпрацювали в оборонних кібероперацією за кілька місяців до вторгнення, щоб посилити кіберстійкість важливі мережі.

З початку вторгнення союзники продовжували зміцнювати онлайн-безпеку України. Наприклад, США та Великобританія поділилися інформацією про російські кібероперації, включаючи дані про кіберзагрози щодо майбутніх та існуючих шкідливих нападів, таких як вірус Industroyer2, захисні брандмауери та захист від DDoS. Крім того, уряд США допоміг Україні знайти та придбати програмне та апаратне забезпечення для посилення захисту мережі. Примітно, що з початку конфлікту Агентство США з міжнародного розвитку (USAID) запропонувало 6750 пристроїв зв'язку для надзвичайних ситуацій, включаючи супутникові телефони та термінали даних, щоб посилити стійкість мереж критичної інфраструктури та уряду. USAID також надало технічних експертів для підтримки постачальників основних послуг. ЄС направив в Україну групу швидкого кібернетичного реагування після того, як Росія вторглася в країну в лютому 2022 року, і виділив Україні 29 млн. євро (приблизно 31 млн. дол.) на посилення її кібер- та цифрового захисту. Крім того, Німеччина виділила частину бюджету на 2023 рік на захист України від російських кібератак.

Через конфіденційність щодо окремих вразливостей повний обсяг кіберактивності Росії проти України та союзників по НАТО не був оприлюднений, хоча спілкування між Україною та її партнерами було двостороннім. Високопоставлені представники кіберзахисту з України також мали двосторонні зустрічі з національними урядами для обміну інформацією, оскільки війна затягується. Союзники, які надали окремих осіб як підкріплення, потім отримують знання, необхідні для кращого захисту своїх власних національних мереж від подібних атак. З приєднанням України до Спільного центру передового досвіду кіберзахисту НАТО в травні 2023 року очікується, що це двостороннє навчання продовжиться, збільшуючи досвід Альянсу шляхом обміну знаннями.

Кіберзахисники з приватного сектору

У російсько-українську війну, окрім традиційних озброєних військ і проксі, залучилися й технологічні корпорації, які є особливо важливими для України. Навряд чи це несподівано, враховуючи, що приватний бізнес контролює та керує більшістю цифрової інфраструктури в Україні. Крім того, давно зрозуміло, що ефективний кіберзахист потребує широкого співробітництва між державним і комерційним секторами. Об'єднана сила приватного сектору покращила обороноздатність України, зокрема її здатність відновлюватися після нападів, підвищила її ефективність на полі бою, дозволила розширити привабливість на міжнародному рівні.

Наприклад, Microsoft, хоч і не єдиний бізнес, який зробив це, відіграв вирішальну роль у захисті України від російських нападів. На початку 2022 року Microsoft виявила троянський кінь Wiper FoxBlade, призначений для фінансових та державних установ України. Корпорація Майкрософт зв'язалася з Енн Нойбергер, заступником радника з національної безпеки США з кібернетичних і нових технологій, після оновлення своїх систем виявлення вірусів, щоб зупинити шкідливий код, і налагодити безпечний канал зв'язку з кіберслужбовцями для підтримки захисту України. Відтоді Microsoft та інші компанії продовжували співпрацювати з урядовими кіберекспертами НАТО, ЄС і США, щоб надати будь-які докази діяльності загроз, які поширюються за межі України.

Хоча Microsoft зробила значний внесок у кібербезпеку України та ширшої спільноти, це лише одна з кількох організацій приватного сектору, які втрутилися, щоб допомогти Україні. Разом із великими внесками окремих організацій, приватний сектор зробив значний внесок в Україну через співпрацю з іншими організаціями для спільного забезпечення кібербезпеки країни. З початку вторгнення Росії група корпоративного сектору та груп громадянського суспільства запропонувала забезпечити та підтримувати надзвичайні потреби України в кібербезпеці.

Зберігання основних даних поза зонами конфлікту

Ініціативи з локалізації даних призвели до концентрації даних українського уряду на серверах, які на початку війни базувалися в країні. Однак через прагматизм з боку України, яка визнала ймовірність атаки на ці сервери, разом із підтримкою приватного сектору для підвищення стійкості дані з України були перенесені на сервери за межі зони конфлікту за допомогою Amazon Web Services (AWS), Google Cloud і Microsoft. Вбудовування резервування в мережі та зберігання даних за межами зон бойових дій є важливими для захисту від нападів, спрямованих на паралізування компаній або даних для захисту від цих атак. Це захищає системи зберігання даних і полегшує подальше відновлення економіки. Зараз існують ініціативи, спрямовані на локалізацію даних у кількох країнах. Досвід України нагадує про необхідність захисту фізичної інфраструктури кіберпростору та, у разі пошкодження, перенесення серверів даних.

Волонтери та хактивізм

Створення добровольчої ІТ-армії України було офіційно оголошено 26 лютого. Український уряд, схоже, певним чином координує її дії. Було створено цю безпрецедентну кіберсилу з понад 150000 добровольців. Федеральна пошта та пенсійний фонд, онлайн-банкінг і платформи для відеоконференцій – це лише деякі з понад 600 онлайн-ресурсів у Росії, на які вплинула ІТ-армія. Хакерська група Anonymous також оголосила кібервійну Росії, взявши на себе відповідальність за DDoS-атаки, які вивели з ладу офіційні сайти Кремля та Міністерства оборони, а також розмістили проукраїнську інформацію на російських державних телеканалах. Незважаючи на нетрадиційність, ця волонтерська група допомогла зміцнити кіберзахист України.

Кампанії впливу та відкритий інтернет

Ця безперервна війна дає важливу інформацію про природу конфлікту в “розколотій мережі”, яка стосується двох або більше мереж Інтернету, які розділені та працюють по-різному. У цьому випадку Україна є частиною більш відкритого середовища даних, тоді як Росія має жорстко регульований інформаційний простір. Наратив на користь Росії на російських інтернет-сайтах. Китай і кілька інших країн приєдналися до Росії, підтримуючи цей наратив. Проте низка операцій впливу була спрямована проти інформаційного простору в Україні, який є складовою більшого, більш відкритого Інтернету.

Війну між Росією та Україною назвали “першою війною TikTok”, що підкреслює вплив соціальних медіа на сучасні війни. Соціальними медіа користуються не лише громадські журналісти в зонах бойових дій, а й особи, які займають владні посади. Президент України Зеленський ефективно використовував соціальні мережі для захисту інтересів України та отримання

підтримки в усьому світі. Російські офіційні ЗМІ використовували ті самі місця для поширення фейкових новин і пропаганди. Meta, Twitter, Microsoft, Alphabet і TikTok видалили фейковий контент зі своїх платформ. Адміністрація Байдена навіть зайшла так далеко, що консультувала впливових осіб TikTok щодо стратегічних цілей США. Незважаючи на те, що соціальні мережі допомогли зменшити поширення дезінформації, графічних зображень і ненависті, проблеми залишаються.

Національні уряди, які виступають за відкритий Інтернет, стикаються зі значними труднощами, оскільки регулювати всі інформаційні потоки неможливо й не бажано, що робить їх більш сприйнятливими до зловмисних спроб вплинути на громадську думку. Крім обов'язків і зобов'язань платформ перед обличчям спроб зловмисного впливу, необхідно також враховувати психологічну стійкість і стійкість особи до цих впливів. Створення соціального психологічного захисту або здатності суспільства колективно протистояти зовнішньому зловмисному впливу та дезінформації, ймовірно, стане інституціоналізованою та розширеною частиною багатьох національних заходів із кіберзахисту в суспільствах, які мають намір підтримувати "вільний і відкритий" Інтернет.

Фінансування союзників у приватному секторі

Приватний сектор був готовий і спроможний допомогти національній обороні України, що відразу позначилося на реальних обставинах. Хоча внески приватного сектору в українську армію були суттєвими, вони також були дорогими. Microsoft інвестувала у війну майже 400 млн дол. і витратить додатково 100 млн дол. на безкоштовні послуги до кінця 2023 року. Згідно з повідомленнями, витрати Starlink на технічне обслуговування становлять 20 млн. дол. на місяць, забезпечуючи Україну необхідною інфраструктурою для підключення до мережі інтернет. За значні кошти Amazon створює резервні копії академічних даних, українського уряду та важливої інфраструктури за межами української території. Поставки російських продуктів і послуг припинила низка американських ІТ-компаній.

Важливо розрізняти дії цих технологічних корпорацій і доброзичливість. Наприклад, наслідки кризи можуть вплинути на компанію Microsoft за межами України; тому вжиття заходів і захист від кібератак відповідає інтересам Microsoft. У більш загальному плані, якщо ці переважно американські технологічні компанії залишаться нейтральними або продовжуватимуть вести бізнес з Росією, вони можуть зіткнутися з регуляторною та суспільною реакцією на значущих ринках США і Європи. Як наслідок, досі існують певні побоювання щодо довгострокової життєздатності цієї допомоги. Тривалість часу, протягом якого ці компанії захочуть і зможуть надавати ці дорогоцінні послуги Україні протягом війни, досі невідома, як і питання про те, чи така підтримка може бути відтворена для будь-якої іншої країни в майбутньому.

Контроль технологій подвійного призначення

Виробник комерційних дронів споживчого класу DJI ненавмисно перетворився на торговця зброєю в цій війні. Комерційні дрони, такі як DJI Mavic 3 вартістю менше 2000 дол., використовували як Росія, так і Україна. Завдяки цим недорогим безпілотникам, які також пропонують покращені можливості розвідки та зв'язку, бойова зона дії української армії була збільшена. Деякі з цих розважальних дронів українська армія навіть переобладнала в безпілотні

бомбардувальники-камікадзе, які можуть наводити на російські цілі та нести до 800 кг боєприпасів. Незважаючи на заяву DJI про припинення продажу дронів Москві та Києву у зв'язку з їх використанням у війні, інші постачальники все ще продають комерційні дрони. Проблема з деякими технологіями подвійного призначення показана на цьому прикладі технології, яка є перш за все комерційними, але мають потенціал для застосування в обороні. Крім того, це викликає занепокоєння щодо того, як певні союзники зможуть отримати порівнянну технологію, яка в основному використовується в обороні, і як можна вирішити ці дві проблеми.

Майбутні промислові вороги

За винятком TikTok і DJI, які належать Китаю, більшість основних компаній споживчих технологій, які беруть участь у цій війні, є американськими. Важливо враховувати й іншу можливість, яка передбачає війну з Китаєм. Через військові дії Росії в Україні більше 30 країн, або більше половини світової економіки, запровадили санкції та обмеження експорту. Ці ініціативи вплинули на розвиток російських технологій та електронної комерції. Вкрай важливо взяти до уваги довгострокові наслідки ескалації розколу технологічних пакетів, який в першу чергу мотивується напруженістю між США та Китаєм, навіть якщо санкції проти російських технологій є доцільними як засіб забезпечення відповідності міжнародній волі. Хоча роздвоєння зменшило б залежність, надзвичайно важливо взяти до уваги потенційні наслідки створення більш фрагментованої глобальної технологічної сцени щодо доступу до ресурсів і прихильності підприємств, які мають міцні зв'язки з конкурентами.

Потрібна відповідальність

В ООН були узгоджені норми відповідальної поведінки держави щодо належного використання кіберможливостей. Країни-члени ООН узгодили 11 кіберправил. Ці норми охоплюють міждержавне співробітництво у сфері кібербезпеки, запобігання зловживанню інформаційними та комунікаційними технологіями на суверенній території, захист критичної інфраструктури від пошкоджень, забезпечення безпеки ланцюга постачання та утримання від втручання в роботу груп реагування на надзвичайні ситуації. Незважаючи на це важливе досягнення, все ще існують проблеми, такі як відсутність відповідальності.

Держави часто використовують кібероперації для досягнення своїх цілей на державному рівні. Проте, враховуючи систему стримувань і противаг на національному та міжнародному рівнях, деякі уряди виявляють більшу стриманість, ніж інші, обмежуючи свої кібероперації або, як висловилася Великабританія, "відповідальну кібервладу". Однак це призводить до ситуації, коли існує група країн (таких як Росія, Китай та Іран), які менш стримані у своїх кібероперациях, створюючи серйозну загрозу для інших країн (таких як Великобританія та США), які дотримуються правових рамок і проявляють стриманість. США та їхні партнери працювали над тим, щоб призначити відповідальність за дії державних суб'єктів в кіберпространстві, що набуло форми приписування. Є кілька випадків, коли державних діячів звинувачували в хакерських атаках і корпоративному шпигунстві. Але, здається, атрибуція не заважає державам поводитися неправильно. Для того, щоб забезпечити відповідальність урядів за дотримання міжнародних стандартів, необхідно

розробити більш ефективні механізми відповідальності та покарання, що зрештою може покращити глобальну кібербезпеку.

Який захист мають волонтери?

Сотні тисяч ІТ-волонтерів підтримували кібероперації проти російської держави в рамках кіберзахисту України, але незрозуміло, чи захищені вони якимось чином міжнародним правом. Міжнародний Комітет Червоного Хреста наводить кілька дій як приклади участі у бойових діях: електронне втручання у військові комп'ютерні мережі; передача розвідувальних даних про тактичне націлювання для конкретної атаки; безпосереднє заподіяння смерті, травми або руйнування третій стороні; або заподіяння прямої шкоди військовим операціям або потенціалу противника. У США чи Великобританії, наприклад, хакери, які беруть участь у кібератаках проти України, можуть порушувати міжнародне право. Таким чином, участь добровольчих кібервійськ з різних географічних місць створює значні труднощі для міжнародних конвенцій і правил, розроблених з урахуванням держав.

Ситуація в Україні має важливі наслідки для світового сектору кібербезпеки. Для кіберстійкості перед лицем зростаючих загроз необхідні значні витрати на захист. Це було відомо ще до вторгнення Росії, але не відразу було очевидно, що кіберзахист України буде таким успішним, як зараз. Що очевидно у випадку України, так це те, що її потужний кіберзахист на сьогоднішній день є прямим результатом майже 10 років, які вона витратила на те, щоб захищати свої національні інтереси в кіберпросторі, що вимагало співпраці між урядом і всім українським суспільством у на додаток до роботи з союзниками та приватним сектором. Стійкість і здатність країни протистояти російським кібер- та інформаційним кампаніям зросла завдяки інвестиціям у кіберзахист, підготовці до гібридної війни, наданню високого пріоритету інформаційній безпеці та вихованню культури кіберобізнаності в суспільстві. Росія, ймовірно, продовжуватиме становити серйозну та постійну небезпеку для багатьох членів західного альянсу. З огляду на це, можна і потрібно багато чого навчитися з минулого досвіду України, щоб допомогти кіберзахисникам мати кращі шанси протистояти ворожим нападам у кіберпросторі. Досі залишається багато проблем без відповіді щодо життєздатності відтворення цього унікального та різноманітного партнерства між союзниками, волонтерами та комерційним сектором у кіберпросторі. Але те, що всі отримають із ситуації в Україні, так це те, що сильний захист може бути таким же успішним, як і сильний напад.

ЩО ТАКЕ ФІШИНГ?

Фішинг – це ряд шахрайських дій, спрямованих на викрадення персональних даних користувачів інтернету та незаконне заволодіння коштів за допомогою отриманої інформації. Назва походить від англійського слова fishing - тобто ловити рибу, або ловити на гачок наївних громадян. Як правило, зловмисники полюють на паролі номери банківських карт, а також на конфіденційні дані клієнтів різних платіжних систем, інтернет-банкінгів та сервісів з надання кредитів онлайн.

Кожного року жертвами фішингу стає все більша кількість людей. Все тому, що схеми шахраїв стають щораз складнішими та удосконаленими, а більшість користувачів не знають та не використовують навіть елементарних правил

інтернет-безпеки.

Крім того, кіберзлочинці не діють по одній і тій же схемі. Сфера їх діяльності максимально розширена, для виманювання цінної інформації хакери застосовують:

- розсилку електронних листів з проханнями переказу грошей на їх рахунки,
- смс-повідомлення із посиланнями на шкідливий веб-сайт або вірусний матеріал,
- матеріали в мережі, замасковані під офіційні джерела,
- копії соціальних мереж або банківських сервісів, де користувач повинен вписати пароль від електронної пошти та назву від справжнього облікового запису користувача.

ФІШИНГОВІ СХЕМИ ШАХРАЙСТВА

Способи роботи хакерів настільки хитрі та продумані, що жертва часто не підозрює обману, поки не виявить порожній банківський рахунок або, що набагато гірше – отримає дзвінок з банку або візит колекторів з вимогою погасити величезний борг. Ось кілька найпоширеніших схем фішерів (так називають кіберзлочинців, які використовують методи фішингу).

ФІШИНГОВІ САЙТИ

Це одна з найдавніших та найпопулярніших схем фішерів та чорних кредиторів. Для виманювання персональних даних шахраї створюють підставні інтернет-магазини з не існуючими товарами, сервіси з надання дистанційних послуг (поповнення мобільних рахунків, продаж електронної продукції: книг, аудіозаписів, відео, програмного забезпечення). Не менш частим явищем являється також створення сайтів клонів відомих брендів, банку або кредитної компанії. Саме через останні зараз стрімко зростає кількість випадків шахрайства в кредитуванні та оформлення кредитів на чужі паспорти.

ФІШИНГОВІ ЕЛЕКТРОННІ ЛИСТИ

Як правило, електронні листи, вислані кібер шахраями, маскуються під повідомлення з офіційних сайтів різних установ: банків, бюро кредитних історій, податкової, чи різних найпопулярніших інтернет-сервісів, де зареєстрований кожен користувач інтернету (Microsoft, Google, Gmail). В таких повідомленнях заміщається текст з проханням, наприклад, пройти актуалізацію профілю або уточнити дані, а також прив’язується посилання на нібито потрібний ресурс, але насправді на обманні сайти або на вірусний файл.

ФІШИНГОВІ СМС-ПОВІДОМЛЕННЯ

Дана схема діє трохи по-іншому, ніж емейл-розсилка, адже жертвам, як правило, пропонують взяти участь в неіснуючих розіграшах або відправити певні дані для отримання виграшу. Як правило, в смс-повідомленнях також вказується посилання, за яким потрібно перейти або телефонний номер, на який потрібно задзвонити. Іноді, в таких смс просять також сплатити кошт доставки призу або інші «суміжні» платежі.

ФІШИНГ В СОЦІАЛЬНИХ МЕРЕЖАХ

Це особливо популярний вид шахрайства останніх років, і, треба сказати, одна з найприбутковіших схем фішерів. Адже затрати на створення різних вірусних матеріалів та злом сторінок користувачів – мінімальні, а результати досить великі. Попри те, що застереження не публікувати особистих даних та фотографій документі, не вказувати геолокацію, адресу проживання, місце

роботи та контактні дані, а також не висилати такої інформації в приватних повідомленнях через соцмереж лунають не одноразово, все ж більшість осіб ігнорують такі заходи безпеки, через що пізніше поносять гіркі наслідки.

ЯК РОЗПІЗНАТИ ТА ЗАХИСТИТИСЯ ВІД ФІШИНГУ?

Хоча фішинг-шахраї використовують досить хитрі схеми виманювання персональних даних, проте є кілька важливих вказівок, які допоможуть розпізнати їх атаки та подбати про захист персональних даних.

- Якщо мова йде про фішингові сайти, то вони не мають безпечного з'єднання, зареєстровані на ненадійних доменах, часто присутня велика кількість граматичних помилок та не завжди коректно працюють усі сторінки сайту. Якщо ресурс представляє інтернет-магазин або сервіс кредитування, то пропозиції, звичайно, набагато нижче ринкової ціни, а після введення реквізитів карти може відбуватися збій операції.
- Щоб захиститися від кредитного шахрайства через використання зловмисниками фішинг-сайтів або від крадіжки грошей зі свого рахунку, краще ніколи не відвідувати підозрілі сайти. Однак, якщо ви відкрили хакерський ресурс та встигли зробити деякі дії, перш ніж помітити небезпеку, негайно покиньте ресурс та очистить кеш-пам'ять комп'ютера, включить повну вірусну перевірку, а також надішліть траур на підозрілий сайт до Державного департаменту кіберполіції.
- Що стосується фішингових атак за допомогою смс та емейл-повідомлень, то розпізнати зловмисників також не важко. Головне пам'ятати, в яких конкурсах ви справді брали участь та звідки чекаєте відповіді, знати або мати записаними офіційні номери банків, в яких обслуговуєтесь та відкривати повідомлення тільки з перевірених осіб чи органів.
- А якщо приходить повідомлення з необхідністю актуалізувати інформацію на одному з ваших акаунтів в соцмережах чи на сайтах програмного забезпечення, то щоб подбати про безпеку персональних даних краще не переходити безпосередньо через вказані посилання, а відвідати потрібний сайт через надійний браузер.

Захист від фішингу

- Не розкривайте особисті дані. Пам'ятайте, що нікому не можна передавати таку конфіденційну інформацію, як PIN-код банківської картки, паролі електронної пошти або облікові записи в соцмережах. Ні банк, ні соцмережа ніколи не запитуватимуть ці дані по e-mail.
- Оновлення програмного забезпечення. Встановіть хороший антивірус із оновлюваною базою. Як правило, у всіх популярних антивірусах є захист від шпигунських програм.
- Будьте обережні. Соціальні мережі та браузери попереджають про перехід на підозрілий сайт. Не ігноруйте такі сповіщення.
- Звертайте увагу на дизайн сайту. Якщо він зроблений нашвидкуруч, містить помилки та викликає підозри, то такий ресурс може виявитися фішинговим.
- Уважно вивчайте адресний рядок. Навіть незначні зміни в URL можуть призвести до абсолютно іншого сайту. Уважно перевіряйте адреси електронної пошти відправників та посилання у листах.
- Будьте обережні зі скороченими посиланнями на кшталт bit.ly, на їхній вигляд неможливо сказати, куди вони вас перенаправлять. Якщо ви отримали листа з

коротким посиланням від невідомого відправника, не відкривайте його, доки не дізнаєтесь, куди воно веде.

- Використовуйте захищене з'єднання. Під час відвідування банківських сайтів та здійснення фінансових операцій в інтернеті слідкуйте, щоб було встановлено захищене з'єднання **https://** . На це вказує буква s перед двокрапкою та значок закритого замка в адресному рядку. При кліку по цьому замку можна перевірити безпеку з'єднання. Звертайте увагу на сертифікат: він має бути дійсним.
- З підозрою поставтеся до електронних листів, які тиснуть на емоції або вимагають якихось термінових дій. Якщо лист починається зі слів «Ваш обліковий запис» або «Ви отримали великий виграш», то в більшості випадків це фішинг.
- Намагайтеся не заходити у свої банківські облікові записи з громадських точок Wi-Fi. В цьому випадку шахраї можуть легко перехопити ваші особисті дані.
- Якщо в листі сказано, що потрібно виконати ті чи інші дії у вашому поштовому, банківському або іншому обліковому записі, не варто заходити туди через посилання, яке прикріплено до листа – воно може вести на підроблену сторінку. Краще вручну введіть адресу офіційного сайту та перевірте інформацію там.
- Використовуйте двофакторну автентифікацію, яка додасть додатковий шар захисту до ваших облікових записів.