# **Модуль 1**

## **Знайомство з ІТ-безпекою**

### **Вступ до курсу**

Перш ніж перейти до наступного курсу, я хочу вас щиро привітати. Ви пройшли непростий шлях до завершального курсу цієї програми. Так, це було нелегко, але погляньте, якого прогресу ви досягли. Ви вивчили всі основи ІТ. Зараз ми на останньому курсі, який доповнить ваші базові знання. Ми поговоримо про безпеку. Без неї всі процеси, які ви вивчили до цього часу, можуть зазнати невдачі, а цього не хоче жоден ІТ-фахівець.

Перш ніж ми перейдемо до справи, ще раз представлюся. Ми зустрічалися ще на першому курсі, коли говорили про історію Інтернету й Інтернет речей. Мене звати Джіан Спікузза, і я керівник програм у відділі безпеки Android. Я допомагаю захищати понад 2 млрд пристроїв Android, випускаючи нові функції безпеки та керуючи ними для кожної версії Android (які мають назви десертів).

Скільки я себе пам’ятаю, я завжди любив техніку. Я працюю у сфері ІТ з 16 років, і на дозвіллі я любив читати книжки про нові технології й збирати сервери зі старих комп’ютерних деталей у підвалі батьківського будинку. Я ніколи не складав тести дуже добре, і доказом тому були мої оцінки. Але це не зупинило мене на шляху до успішної кар’єри. Я працював єдиним ІТ-спеціалістом на три некомерційні організації, поки здобував освіту. Це був ще той стрес – відповідати за все: від налаштування й адміністрування баз даних до навчання нових працівників роботі з електронною поштою та внутрішніми інструментами.

Озираючись назад, я розумію, що цей досвід був безцінним. І, звісно, важливою частиною моєї роботи у сфері ІТ була саме безпека. Тепер я працюю безпосередньо з виробниками обладнання, розробниками додатків і командами інженерів у Google, забезпечуючи найвищий рівень захисту для наших користувачів. Для багатьох із них мобільний телефон – це єдиний спосіб зв’язку з Інтернетом. І я відчуваю велике задоволення, знаючи, що моя робота суттєво впливає на людей в усьому світі, які так покладаються на свої пристрої. Щоб досягти успіху в кібербезпеці, іноді потрібно подумки поставити себе на місце нападника й завжди бути на крок попереду. Отже, ви готові робити добро, думаючи про погане? Тоді поїхали!

Цей модуль буде повністю присвячений питанням безпеки: як безпеку намагаються порушити та як ми захищаємося від цих атак. Наприкінці цього модуля ви зможете визначати й розпізнавати ризики, вразливості й загрози безпеці. Ви також зможете визначити найпоширеніші атаки на системи безпеки. Нарешті, ви зрозумієте, як безпека обертається навколо принципу КЦД, і що таке принцип КЦД.

Коли йдеться про безпеку, що найперше спадає вам на думку? Мабуть, це фізична безпека, щось на кшталт захисту майна від потенційних злодіїв, зачинення вхідних дверей уночі та зберігання цінних речей у безпечному місці. Але в сучасному цифровому світі гроші зберігаються не лише в гаманці. Кошти також зберігаються на банківських рахунках онлайн, до яких можна отримати доступ, знаючи пароль. Дехто з нас узагалі не носить із собою кредитних карток, а якщо й носить, то не в гаманці. Вони зберігаються на наших улюблених вебсайтах, щоб зручніше робити покупки.

Але ми турбуємося не лише через гроші. Більша частина нашого особистого світу зберігається на мобільних телефонах. SMS-повідомлення, фотографії, особисті дані, дані для входу в додатки й багато іншого – усе це зберігається всередині пристроїв, які ми носимо в кишенях. На жаль, ми живемо у світі, у якому деякі люди й організації намагаються викрасти дані в компаній, урядів і навіть простих людей, як ми з вами. Однак фільми дають спотворене уявлення про цих цифрових злодіїв. Вони не такі гламурні чи професійні, як вам може здаватися. Цифрові злодії не мають команди хакерів, не носять темні худі й не друкують несамовито на своїх терміналах цілими днями, сподіваючись зламати системи багатомільярдних компаній. Я не кажу, що такого не трапляється, – нам усім відомі такі випадки. Але зазвичай середньостатистичний інтернет-зловмисник має такий самий вигляд, як ми з вами, – це звичайна людина, яка випадково дізналася про діру у вашій системі безпеки, а потім нею скористалася.

Наприклад, злодій міг просто дізнатися, що ваш пароль – це кличка вашої собаки. Коли єдине, що захищає ваш банківський рахунок, – це слово Fido, у вас проблеми. Але так само, як фізичні пристрої сигналізації стримують потенційних грабіжників, існує також чимало способів запобігти порушенню нашої цифрової безпеки. У цьому курсі ви глибше зрозумієте комп’ютерну безпеку. Ви дізнаєтеся, як запобігти найчастішим комп’ютерним атакам. Ви зрозумієте різні протоколи й механізми безпеки, які використовуються на наших комп’ютерах, в Інтернеті та в наших мережах. Ви також більше дізнаєтеся про криптографію, автентифікацію й механізми доступу, що є важливими навичками для фахівця з ІТ-підтримки. Наприкінці курсу ми дамо вам необхідні інструменти для оцінки безпеки в організації та визначення оптимальних запобіжних заходів для її захисту.

Сьогодні майже кожна компанія або галузь значною мірою покладається на технології для ведення повсякденного бізнесу. Чи можете ви уявити собі компанію (велику чи малу), яка б працювала без електронної пошти, функціональних комп’ютерів чи Інтернету? Візьмімо, наприклад, маленьку компанію. Їй потрібні певні технології для доступу до кредитних карток. Нещодавні атаки, як-от крипточерв’як WannaCry і масштабні атаки з використанням бот-мережі Mirai, унаочнюють обсяг і масштаб того, як безпека впливає на всіх нас. До цього питання слід ставитися серйозно. Через нашу широку залежність від технологій цифрова безпека важливіша, ніж будь-коли раніше, і її вплив лише зростатиме в усіх галузях і аспектах нашого життя. Тож зробімо так, щоб ви були озброєні належними інструментами для захисту себе й своїх майбутніх клієнтів.

## **Шкідливе програмне забеспечення**

### **Тріада CIA**

Протягом усього цього курсу ми часто вживатимемо одну ключову абревіатуру – "КЦД" (англ. – CIA). Ні, я говорю не про Центральне розвідувальне управління США (теж CIA), хоча воно багато робить для національної безпеки. У нашому випадку "КЦД" означає "конфіденційність, цілісність і доступність". Ці три ключові принципи є основою того, що зазвичай називають "тріадою КЦД". Це керівна модель для розробки правил інформаційної безпеки. Ці три принципи допоможуть вам розробити правила безпеки на робочому місці та у ваших особистих середовищах.

Почнімо з конфіденційності. Конфіденційність означає зберігання в таємниці. В IT це означає зберігання наявних даних надійно прихованими від сторонніх очей. Один із методів конфіденційності, який ви напевно використовуєте щодня, – це захист паролем. Лише ви і ще, можливо, ваш партнер маєте знати пароль для доступу до банківського рахунку онлайн. Для забезпечення конфіденційності потрібно обмежити доступ до даних. Знати, як отримати доступ, мають лише ті, кому це абсолютно необхідно.

Літера "Ц" в абревіатурі "КЦД" означає цілісність. Цілісність – це збереження даних точними й неспотвореними. Дані, які ми надсилаємо чи отримуємо, мають залишатися незмінними протягом усього процесу. Уявіть, що ви завантажили файл з Інтернету. На вебсайті, з якого ви його завантажили, указано, що розмір файлу – 3 МБ. Але після завантаження виявилось, що справжній розмір файлу – 30 МБ. Це сигнал про небезпеку. Щось сталося під час завантаження, щось потенційно небезпечне. Можливо, на вашому жорсткому диску тепер існує небажаний файл. Як ви дізнаєтеся на наступних уроках, таке трапляється дуже часто.

І останнє, але не менш важливе. Літера "Д" у "КЦД" означає "доступність". Доступність означає, що наявна інформація легко доступна тим користувачам, яким вона необхідна. Це може означати багато речей, зокрема готовність до втрати даних або збою системи. Хакерські атаки мають на меті вкрасти у вас чимало речей: час, матеріальні цінності, вашу гідність. Іноді у вас крадуть час, який ви мусите витрачати на відновлення роботи сервісів. Деякі зловмисники утримують вашу систему в заручниках, доки ви не заплатите викуп. Звучить страшно, і насправді так і є. Але саме тому ви тут – щоб дізнатися, як не допускати подібних атак.

Протягом цього курсу ви дізнаєтесь, як кожний аспект безпеки пов’язаний із цими трьома ключовими принципами: конфіденційністю, цілісністю та доступністю.

### **Основні умови безпеки**

Перш ніж докладно розглянути, як зупиняти цифрових злодіїв,

прояснімо деякі терміни.

Ми будемо використовувати ці терміни протягом усього курсу,

тож їх слід добре зрозуміти.

Перший термін – "ризик".

Це – можливість зазнати збитків у разі атаки на систему.

Скажімо, ви купуєте новий телефон.

Один із заходів безпеки для захисту вашого пристрою –

налаштувати блокування екрана за допомогою пароля або ключа,

щоб запобігти доступу інших осіб до ваших даних.

Блокування екрана – це функція безпеки, що допомагає запобігти

небажаному доступу шляхом створення дії, яку потрібно виконати, щоб увійти.

Якщо ви вирішите не блокувати екран телефона,

ви піддаєте себе ризику того, що хтось може легко

отримати до нього доступ і викрасти ваші дані.

Навіть просте додавання пароля чи блокування екрана може допомогти

захистити ваші особисті дані або дані компанії

від потрапляння до сторонніх осіб.

Наступний термін – "вразливість".

Це недолік у системі, який можна використати, щоб її зламати.

Вразливостями можуть бути прогалини, про які ви можете знати чи ні.

Ви можете їхати в тривалу відпустку

й зачинити всі двері та вікна у своєму будинку перед виходом.

Але ви забудете зачинити вікно ванної кімнати.

Тепер це вікно ванної кімнати – вразливість,

яку грабіжники можуть використати, щоб проникнути у ваш будинок.

Інший приклад: скажімо, ви створюєте додаток і активували обліковий запис

для тестування під час розробки,

але забули вимкнути його перед запуском додатка.

Тепер у вашому додатку є вразливість, яку потенційно може виявити зловмисник.

Є особливий тип вразливості, що називається

"вразливість нульового дня".

Це вразливість, яка не відома розробнику або постачальнику

програмного забезпечення, але відома зловмиснику.

Назва означає кількість часу, яку мав постачальник програмного забезпечення,

щоб зреагувати й усунути вразливість, а саме "нуль днів".

Ще один ключовий термін – "експлойт".

Це програма, за допомогою якої використовується

вада безпеки чи вразливість.

Зловмисники створюють експлойти для вразливостей,

які знаходять у ПЗ, щоб заподіяти шкоду системі.

Скажімо, зловмисниця виявляє вразливість нульового дня.

Вона вирішує скористатися раніше не відомою вадою

та пише код експлойту нульового дня.

Цей код буде спрямований на використання цієї конкретної невідомої вади,

щоб отримати доступ до систем і заподіяти їм шкоду.

Не надто приємна новина.

Наступний важливий термін – "загроза".

Це ймовірність небезпеки, яка може використати вразливість.

Загрози – це просто можливі зловмисники, свого роду грабіжники.

Не всі грабіжники намагатимуться проникнути у вашу оселю,

щоб викрасти найцінніші речі,

але вони можуть це зробити, а тому вважаються загрозами.

Наступний термін – "хакер".

У світі безпеки це той, хто намагається проникнути в систему чи використати її.

Більшість із нас асоціює термін "хакер" зі зловмисниками.

Але насправді є два поширені типи хакерів.

Є так звані "чорні хакери",

які намагаються проникнути в системи, щоб зробити щось шкідливе.

Але є й "білі хакери", які намагаються знайти слабкі місця в системі,

але при цьому попереджають власників цих систем,

щоб вони могли виправити ситуацію, перш ніж хтось інший заподіє шкоду.

Існують й інші типи хакерів,

але ці два – основні й найважливіші для нас зараз.

Останній термін, який потрібно знати, – "атака".

Це – фактична спроба заподіяти шкоду системі.

Дуже важливо усвідомлювати можливі загрози й вразливості системи,

щоб мати змогу краще підготуватися до атак.

Сумна реальність полягає в тому, що атаки на вашу систему будуть завжди.

Але перш ніж почати пошук підземного сховища,

щоб провести там решту своїх днів,

подумайте про те, що існують способи виявляти та пом’якшувати атаки,

і ми допоможемо вам навчитися це робити.

У цьому модулі ми поговоримо про деякі найпоширеніші типи атак,

які траплятимуться вам вдома й на роботі.

На цьому курсі ви дізнаєтеся, як убезпечити свої системи від цих атак.

Виявляється, існують сотні способів атакувати вашу систему.

Але також існують і сотні способів запобігти їм.

Ми розглядатимемо не всі, а лише найважливіші з них.

Тож відкиньте ідею з бункером і приготуйтеся до нових знань,

бо ми говоритимемо про реальні речі – реальну безпеку.