УДК 004.056.56:342(043.2)

В. Морозов, В. Святненко,
О. Туровський, д.т.н., професор.
(Національний авіаційний університет, Україна)

Кіберзлочини та способи захисту від них

Кіберзлочини є серйозною загрозою для сучасного суспільства, зокрема в контексті широкого використання інтернет-технологій та зростання кількості кібератак. Метою цього дослідження є визначення основних видів кіберзлочинів, вивчення їх впливу на різні сфери діяльності та розгляд можливих способів захисту від них.

У роботі було проведено огляд літератури з питань кіберзлочинів, зокрема їх класифікації та типології. Були визначені основні види кіберзлочинів, такі як крадіжка даних, шахрайство, фішинг, розповсюдження шкідливих програм тощо, а також розглянуто можливі наслідки кібератак, такі як втрата даних, фінансові втрати, порушення конфіденційності та інші.

Далі в роботі були проаналізовані різні підходи до захисту від кіберзлочинів, такі як використання антивірусного програмного забезпечення, фаєрволів, мережевих заходів безпеки, шифрування даних, багаторівневої аутентифікації та інших заходів. Окрему увагу було приділено питанням кібербезпеки на рівні користувача, оскільки багато кіберзлочинів мають соціальний аспект та вимагають свідомої кібергігієни.

Висновки роботи підтверджують важливість проблеми кіберзлочинів та необхідність впровадження комплексного підходу до захисту від них. Результати дослідження вказують на те, що захист від кіберзлочинів має включати не лише технічні заходи, такі як використання захисного програмного забезпечення, але й навички кібергігієни та свідомість користувачів. Додатково, організації повинні розробляти політики кібербезпеки та впроваджувати механізми моніторингу та виявлення кіберзлочинів.

Із початком військової агресії росії на території України громадяни держави зіткнулись з великою кількістю кібератак у вигляді посилань на фішингові сайти які могли пограбувати у користувача інтернету логіни та паролі від соцмереж, банківських карток, особисті дані та фото, та ще безліч особистої інформації.

До найпоширеніших видів кіберзлочину відноситься фішинг, кардинг, онлайн шахрайство, та соціальна інженерія. Для того щоб розуміти як звичайний користувач інтернету може запобігти та захистити себе потрібно розібратися та зрозуміти кожен вид кіберзлочину, на чому він базується та як відбувається вся схема обману жертви. Почнемо з фішингу.

Фішинг - виманювання у користувачів інтернету їх логінів та паролів до електронних гаманців, соцмереж, хмарних сховищ інформації, сервісів онлайн аукціонів, переказування або обміну валюти, тощо. Весь процес фішингу полягає в тому що це відбувається шляхом відправки на електронну пошту, повідомлень у соціальних мережах або текстових повідомлень, які виглядають так, ніби вони від

імені довірених осіб або організацій, таких як банки, платіжні системи, соціальні мережі, що є елементом соціальної інженерії про яку я розповім згодом. Вам приходить текст з посилання на сайт який виглядає як сторінка соцмережі або будь якого інтернет ресурсу де вам необхідно ввести логін та пароль але в дійсності цей сайт лише виглядає як сторінка соцмережі, насправді цей сайт належить шахраю який хоче у вас виманити інформацію, це може бути не тільки логін і пароль а наприклад особиста інформація така як наприклад ПІБ, вік, стать яка може бути використана в будь яких цілях.

Соціальна інженерія - це наука, що вивчає людську поведінку та фактори, які на неї впливають. Знаючи як людина веде себе в певній ситуації та деяку інформація про людину шахрай цим зловживає. Таким чином в Україні було розповсюджене шахрайство коли людям похилого віку телефонували вночі та представлялися їх сином або дочкою та казали що потрапили у халепу(наприклад ДТП) і терміново потрібні гроші на вирішення цієї проблеми, називали певну суму грошей та давали карту куди людина скинула гроші та вони попадали на рахунок шахрая. Таким чином знаючи номер телефону, сімейний стан людини та ім'я членів сім'ї шахрай має змогу оволодіти певною сумою грошей.

Кардінг - процес отримання несанкціонованого доступу до кредитних або дебетових карток та використання їх для незаконних операцій. Процес кардінгу включає в себе використання різноманітних методів для отримання відкритої або викраденої інформації про кредитні картки (номер картки, термін придатності та код безпеки). Одним з таких методів є використання скімерів (пристрій для зчитування) – який встановлюються в банкомати або в інші платіжні термінали, щоб красти дані картки, зчитуючи їх. Також зловмисники можуть використовувати шпигунське програмне забезпечення, яке встановлюється на портативні пристрої (ноутбуки, смартфони, саморобні пристрої), для викрадення даних картки. Коли зловмисники отримують дані картки, вони можуть її використовувати для подальших операцій в інтернеті або інших фізичних операцій, шляхом створення власної фізичної картки, вже з даними вашої картки.

Онлайн-шахрайство - це вид інтернет-шахрайства, який полягає в тому, що злочинці використовують інтернет, щоб вводити в оману людей і отримувати з цього прибуток. Основними методами шахрайства є шахрайство через електронну пошту, онлайн ігри, соціальні мережі, онлайн аукціони та шахрайство з використанням фальшивих веб-сайтів. Наприклад злочинці можуть відправити вам на електронну пошту лист від імені банку яким ви користуєтесь з проханням надати певну інформацію або зробити платіж. У онлайн-іграх шахраї можуть використовувати навички в соціальній інженерії для отримання певної особистої інформації про гравців або для отримання певної суми грошей, обіцяючи їм виграш, якого ніколи не буде. Останнім часом, зловмисники почали використовувати новий метод шахрайства, який полягає в використанні фальшивих веб-сайтів популярних компаній для продажу товарів або послуг, вони можуть вимагати передоплату від користувача за товар, який ніколи не побачать.

Існує декілька способів захистити себе від кіберзлочинців. Ось кілька рекомендацій:

- встановлюйте антивірусне програмне забезпечення та забезпечувати його регулярну оновлення. Це допоможе виявляти

та блокувати шкідливі програми, які можуть пошкодити ваш комп'ютер або викрасти вашу особисту інформацію.

- використовуйте складні паролі та змінювати їх регулярно. Використання простих паролів може зробити ваші облікові записи вразливими для зламування.
- не відкривайте підозрілі електронні листи та не клікайте на посилання від невідомих вам відправників. Це може призвести до інфікування вашого комп'ютера шкідливим програмним забезпеченням.
- використовуйте двофакторну аутентифікацію для ваших онлайн-облікових записів, якщо це можливо.