**УДК 327.84:004**

**Олексій Георгійович Барбашов,**
*курсант 4 курсу факультету № 4*
*Харківського національного університету внутрішніх справ*

**Денис Олександрович Грищенко,**
*старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ*

# Щодо заходів безпеки для запобігання кіберзлочинності

Протидія кіберзлочинності є сьогодні одним з першочергових завдань, яке стоїть перед правоохоронними органами не тільки України, але й світу. Практика засвідчує, що названий напрям злочинної діяльності перебувають в активній фазі розвитку. Більшість випадків кіберзлочинів виконуються за допомогою відомих уразливостей безпеки, таких як застаріла операційна система та відсутність антивірусних програм для початку атаки. Існує багато різних типів кіберзлочинів, більшість із яких здійснюються з очікуванням фінансових вигод зловмисників, незважаючи на те, що методи, які використовуються кіберзлочинцями для виплат, можуть відрізнятися. Деякі з цих типів кіберзлочинності включають:

Криптовалюта: Ці атаки використовують скрипти для видобутку криптовалют у веб-переглядачах без відома користувача. Атаки криптовалюти можуть мати справу з завантаженням програмного забезпечення для видобутку криптовалют у систему жертви. Однак кілька атак покладаються на код JavaScript, який здійснює майнінг в браузері, якщо в браузері користувача на шкідливому сайті відкрито вікно або вкладку.

Кіберешпіонаж: це трапляється, коли кіберзлочинці втручаються в мережі чи системи, щоб отримати доступ до конфіденційних даних, що належать уряду чи іншим подібним організаціям. Діяльність кіберресурсів може очікувати, що кожен тип кібератаки збирає, коригує або знищує дані, окрім використання підключених до мережі пристроїв, таких як камери чи вебкамери, шпигує за цільовою групою або окремими

особами та контролює комунікації, включаючи текстові повідомлення, миттєві повідомлення та електронну пошту.

Наведемо деякі ключеві кроки для зміцнення безпеки в мережі:

Зміцніть домашню мережу. Настійно рекомендується почати із сильного пароля шифрування та віртуальної приватної мережі (VPN). VPN може зашифрувати весь трафік, залишаючи ваші пристрої, поки він не прибуде до місця призначення. Навіть якщо кіберзлочинцям вдасться зламати вашу лінію зв'язку, вони не перехоплять нічого, крім зашифрованих даних. Завжди корисно використовувати VPN, коли ви користуєтесь загальнодоступною мережею WiFi.

Використовуйте надійні паролі. Ніколи не повторюйте свої паролі на різних сайтах і не змінюйте їх регулярно. Створіть складні паролі, комбінуючи щонайменше 10 букв, символів та цифр. Використання програми керування паролем допоможе зберегти ваші паролі.

Постійно оновлюйте програмне забезпечення. Оновлення програмного забезпечення особливо важливе для Вашого програмного забезпечення безпеки в Інтернеті та операційних систем.

Досягнення позитивних результатів у сфері протидії кіберзлочинності є абсолютно неможливим без відповідної профілактичної роботи серед населення та інформування суспільства про нові види кіберзагроз. При цьому вказані функції повинні реалізовуватися не тільки правоохоронними органами, а й громадськими організаціями масштабу Transparency International, Greenpeace, Amnesty International тощо.

Наостанок відмітимо, що кіберзлочинність – проблема XXI століття, яка невпинно зростає та поглинає все більше фінансових ресурсів. Незважаючи на заходи, що вживаються окремими особами, як фізичними, так і юридичними, державою, це явище продовжує існувати та розширює масштаби своєї діяльності, збільшуючи прибутки правопорушників.

*Одержано 22.10.2019*