Михайленко В. В.,
студент 6 курсу, 3 групи, Господарсько-правового факультету Національного юридичного університету імені Ярослава Мудрого

ОКРЕМІ ПИТАННЯ ВІКТИМОЛОГІЧНОЇ ПРОФІЛАКТИКИ КІБЕРЗЛОЧИНІВ

Ключові слова: кіберзлочини, віктимологічна профілактика, віктимологія, інтернет-злочини.

Анотація. У тезах розглянуто сучасні підходи до кримінологічної профілактики по відношенню до кіберзлочинів. Визначено ключові фактори, що впливають на розвиток відповідного напряму.

Аннотация. В тезисах рассмотрены современные подходы к криминологической профилактике в отношении киберпреступлений. Определены ключевые факторы, влияющие на развитие соответствующего направления.

Ключевые слова: киберпреступления, виктимологическая профилактика, виктимология, интернет-преступления.

Summary. Theses consider modern approaches to criminological prevention in relation to cybercrimes. The key factors influencing the development of the respective direction are identified.

Keywords. Cybercrimes, victimological prevention, victimology, Internet crimes.

Сьогодні поширення інформації не викликає проблем у жодної з верств населення. Завдяки інтернету можливість долучитися до певних заходів, отримати важливі відомості чи новини є реальною для всіх і кожного. Однак, такий високий рівень свободи обігу інформації має і зворотній бік.

Негативним аспектом сучасної високотехнологічної ери є кіберзлочинність, або - злочинність у мережі інтернет. Теперішній підхід до такого роду злочинів може ввести в оману навіть досвідчених чи середнього рівня користувачів, і, звичайно, такі групи як літні люди, або ж підростаюче покоління не завжди можуть без зайвих складнощів розпінити ознаки шахрайських схем. Судячи ж з останнього досвіду масштабних кібератак, що переслідували корисливу мету, у зоні ризику може опинитись кожен [1].

Саме з вищеописаних причин, все більш важливого значення набувають профілактичні заходи, основною ціллю яких є попередження виникнення відповідних ситуацій і недопущення потрапляння довірливих користувачів у тенета зловмисників. У загальному плані даний напрям можна назвати – віктимологічна профілактика кіберзлочинів.

У наукових джерелах зустрічається відповідне тлумачення віктимологічної профілактики як комплексу заходів зі зниження індивідуальної віктимності особи та зменшення масштабів віктимізації населення. Віктимологічна профілактика включає: роз'яснювально-просвітницьку роботу з особами, що входять до групи віктимогенного ризику; заходи індивідуальної і майнової безпеки; організаційно-управлінські заходи, спрямовані на скорочення віктимності громадян; відшкодування шкоди потерпілим від насильницьких злочинів тощо [2, с.159].

Однак, з ходом технологічного прогресу змінилися не лише засоби, використовувані злочинцями, а й трансформувався підхід до боротьби зі злочинною діяльністю у даній сфері.

По-перше, серед засобів роз'яснення та інформування дедалі більшу роль та активну участь почали приймати інтернет-ЗМІ: канали та профілі у соц. мережах, що містять застережливі відомості відносно нових підозрілих активностей у мережі; сайти, котрі

тлумачать та роз'яснюють шляхи боротьби з оманливими відомостями (як перевірити, що запитати, на що звертати увагу в першу чергу) тощо.

По-друге, усталеною практикою останніх років є використання засобів захисту особистої інформації користувачів накшталт двофакторної автентифікації. Використовуючи подібні механізми, при здійсненні операцій з веб-сервісами чи мобільними- або інтернет-додатками користувач може забезпечити безпеку власного профілю та облікових даних і в рази ускладнити доступ до них інтернет-шахраям.

Варто зазначити, що у більшості своїй відповідні заходи носять роз'яснювально-просвітницький характер. На сьогоднішній день засобів, що прямо дозволили б впливати на безпеку користувачів мало і вони мають більш технічну спрямованість та можуть мати місце лише у практиці кожної окремо взятої компанії, яка сама має забезпечити відповідний безпековий рівень.

Однак, існують технічні підходи, що дозволяють самим користувачам захиститись від злочинних посягань у даному контексті. Тут мова йде про спеціальні механізми контролю та додатки, які по аналогії з «батьківським контролем» перевіряють сайти на предмет їх підозрілості, блокують небажані повідомлення та попереджають користувачів про потенційні ризики [3].

Тож, наразі, незважаючи на стрімкий розвиток напрямку кіберзлочинності, звичайні, побутові користувачі мають певну кількість можливостей для самозахисту і, за умови врахування важливих відомостей із кібербезпеки та їх безпосереднього застосування можуть дієво протистояти злочинним посяганням.

ЛІТЕРАТУРА:

1. Пивоваров В. В. Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання / В. В. Пивоваров, С. Ю. Лисенко // Право і суспільство. – 2016. – № 3, ч. 2. – С. 177–182.

2. Кримінологія: підручник / Б. М. Головкін, В. В. Голіна, О.Ю. Шостко та ін; за ред. Б. М. Головкіна. – Харків :Право, 2020. – 384 с.

3. Головкін Б. М. Теперішнє і майбутнє кримінології / Б. М. Головкін // Проблеми законності. – 2020. – Вип. 149. – С. 168–184. URL: http://plaw.nlu.edu.ua/article/view/200724/205532

Науковий керівник: к. ю. н., доц. В.В. Пивоваров