УДК 004.056

Сайчук А.А.[1]
Національний авіаційний університет

Дослідження ролі та місця кіберполіції в системі забезпечення кібербезпеки України

В сучасному світі простежується тенденція виникнення нового типу правопорушень – кіберзлочинів. Це пов'язано з тим, що теперішнє суспільство активно використовує Інтернет-мережі, банківські рахунки, електронні чіпи. Та, незважаючи на таку прогресивність, лишається незахищеним суб'єктом у великому інформаційному просторі.

Мета даного дослідження - розкриття проблем доволі нового напряму інформаційної безпеки - кібербезпеки, виявлення основних вразливих місць та загроз в кіберпросторі та системах, що його реалізують, підтвердження важливості створення кіберполіції для протидії кіберзлочинам.

Основна частина дослідження. Багато осіб користуються сайтами знайомств, соціальними мережами, де процедура реєстрації є досить простою. Люди лишають свої особисті дані на неперевірених сайтах, не задумуючись про наслідки. В цьому полягає один з видів небезпеки – часто люди, зареєстровані на сайтах знайомств виявляються не тими, за кого себе видають. Зазвичай це досвідчені шахраї, які здатні скласти психологічний портрет особи і використовувати в подальшому його в своїх цілях. Наслідками такого можуть стати різні небажані ситуації, наприклад, виманювання коштів у потерпілого, граючи на жалості, або шляхом шантажу. Основне призначення кіберполіції полягає саме у запобіганні, а також протидії таким злочинам.

В перелік завдань кіберполіції входить протидія зазначеним кіберзлочинам та загрозам: скімінг – протизаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток; кеш-трепінг – викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки; кардінг – протизаконні фінансові операції з використанням платіжної картки або її реквізитів, які не ініційовані або не підтверджені її держателем; несанкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування; фішинг – виманювання у користувачів Інтернету їх паролів та логінів; онлайн шахрайство – заволодіння коштами громадян через Інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку; кардшарінг – надання незаконного доступу до перегляду супутникового та кабельного ТБ; соціальна інженерія – технологія управління людьми в Інтернет просторі; мальваре – створення та розповсюдження вірусів та шкідливого програмного забезпечення; рефайлінг – незаконна підміна електронного трафіку. Наведені загрози (вразливі місця в системі безпеки кіберпростору) можна реалізувати за рахунок наявності відповідних знань та компетенцій в області використання

[1] *науковий керівник - к.т.н. Гізун А.І.*

інформаційно-телекомунікаційних систем, в сфері психології, наявності досвіду роботи з шкідливим програмним забезпеченням [4].

Ще одним аспектом діяльності кіберполіції є культурна сфера. Багато років Україна займала перші місця у світі в сфері піратства. Багато творчих об'єднань та організацій працюють із кіберполіцією з початку її створення. Як зазначають представники асоціації музичної індустрії: "Без кіберполіції боротися з піратством неможливо. Всі правоохоронці відмічають, що тільки там, де налагоджена співпраця з правовласниками, є суттєвий результат" [3].

Перший етап створення кіберполіції в Україні проходив в Харкові. Саме там випустили перших кіберполіцейських, серед яких 78 чоловіків і 6 жінок. Процес підготовки тривав 4 місяці, навчальна програма включала в себе не лише теоретичну частину, але й давала змогу оволодіти практичними навичками. Усі слухачі даного напряму мають вищу освіту, 20 з яких юридичну, інші мають досвід роботи у силових структурах України або є учасниками бойових дій на окупованих територіях України та зоні АТО [1,2].

Зараз в кіберполіцію йде набір інспекторів та спецагентів інформаційних технологій, задачею яких стане захист користувачів в віртуальному просторі та надання поліцейської допомоги в режимі реального часу.

Недоліками в роботі кіберполіції можна назвати відсутність належного досвіду та практичних навичок у більшості працівників. Крім того, слідвідзначити деякі інституціональні та організаційні неузгодженості в системі управління кіберполіцією як державним правоохоронним органом.

Незважаючи на високу популярність сучасних технологій, люди не вміють себе захищати в інформаційному просторі. Функція кіберполіції полягає саме у захисті населення від кіберзлочинів, основні з яких розглянуті під час проведення дослідження, та їх запобіганні. Були виділені основні особистісні характеристики типових порушників безпеки в кіберпросторі, за рахунок яких можлива реалізація певних видів кіберзагроз. Досвідчений шахрай може швидко втертися в довіру жертві та заподіяти їй шкоду матеріального або іншого характеру. Оскільки кіберполіція виконує великий перелік завдань у зазначеній сфері, то її створення відбувалося поступово, учасники (нині працівники штату) відбиралися ретельно з проведенням відповідної теоретичної та практичної підготовки. Однак якість самої підготовки і особливості організаційно-управлінської структури не зовсім відповідають міжнародним стандартам даної галузі.

Список використаних джерел

1. *Смичик С. Кіберполіція. Подав заявку. Онлайн дописи [Електронний ресурс] / С. Смичик — 2015. — Режим доступу : http://smychnyk.name/osobyste/podav-zayavku-v-kiberpolitsiyu.html;*
2. *У Харковівипустилипершихкіберполіцейських [Електроний ресурс] // Новини. 5 канал. – 2016. – Режим доступу :http://www.5.ua/suspilstvo/u-kharkovi-vypustyly-pershykh-kiberpolitseiskykh-120251.html;*
3. *Воробйов І. Українська поліція закрила другий у світі торрент – трекер[Електронний ресурс] / І. Воробйов – 2016. – Режим доступу : http://tsn.ua/ukrayina/ukrayinska-kiberpoliciya-zakrila-drugiy-u-sviti-torrent-treker-794693.html;*
4. *Кіберполіція (крок реформі) [Електроний ресурс] // Новини. Українська правда. – 2016. – Режим доступу : http://blogs.pravda.com.ua/authors/avakov/561a92c183c27/.*