Кіберполіція та кіберзлочинність в Україні

Коптяєва А.Ю.
студентка 1 курсу ЮД-744 ДДУВС
Махницький О.В.
науковий керівник, старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

Кіберполіція — територіальний орган Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, хакерами, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Має на меті попередження, виявлення припинення та розкриття кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких, передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем. На жаль на сьогодні комп’ютерні злочини - це одна з найдинамічніших груп злочинців їх чисельність збільшується щогодини [1].

Кіберполіція має певні завдання, щоб досягти конкретні цілі. Наприклад:

1) Реалізація державної політики у сфері протидії кіберзлочинності.

2) Завчасне попередження населення про появу новітніх кіберзлочинів.

3) Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.

4) Швидка реакція на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів.

5) Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.

6) Залучення до міжнародних операціях та співпраць у реальному часі. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.

7) Протидія кіберзлочинам [2].

Кіберзлочинність — це злочин через інтернет. Він включає різні види злочинів, які здійснюються завдяки таким ресурсам, як інтернет та комп'ютер. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація будь-яких персон. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні. Адже ці злочинці можуть анулювати світові рахунки, від цього страждають сотні людей, адже зараз великий відсоток людей зберігає велику суми в банках [3].

Об'єктом кіберзлочинів стає звичайний користувач інтернету будь-якого віку.

Види злочинів [3]:

Кардинг - використання в злочинних операціях реквізитів платіжних карт осіб, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів.

Фішинг - вид шахрайства, при якому до клієнта платіжних систем надсилають повідомлення електронною поштою або повідомленням на телефон нібито від адміністрації або служби безпеки, від банку цієї системи з проханням вказати свої рахунки та паролі для встановлення.

Вішинг - вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний номер, а при розмові запитуються конфіденційні дані власника картки.

Онлайн-шахрайство - несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

Піратство - незаконне розповсюдження інтелектуальної власності в Інтернеті.

Кард-шарінг - надання незаконного доступу до перегляду супутникового та кабельного ТУ. Соціальна інженерія - технологія управління людьми в Інтернет-просторі.

Мальваре - створення та розповсюдження вірусів і шкідливого програмного забезпечення.

Протиправний контент - контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

Рефайлінг - незаконна підміна телефонного трафіку.

Є поради, як не попасти на гачок кіберзлочинців [4] :

1) надійні паролі, а не визначні дати власного життя;

2) встановлювати захист на техніку, такі як блокування, антивірус;

3) перевірка власних облікових записів.

Отже, кіберполіція є головним протистоянням кіберзлочинцям. Є багато методів, які допоможуть уникнути махінацій, головне вчасно ними скористатися. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній. Нині кіберзлочинність становить для нашої держави більш серйозну небезпеку, ніж ще 5 років тому. Незважаючи на зусилля правоохоронних органів, спрямованих на боротьбу з кіберзлочинами, їх кількість, на жаль, не зменшується, а, навпаки, постійно збільшується. Треба багато сил, знань та фахівців, щоб хоч якось призупинити цей вид злочину. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців.

1. https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B0)

2. https://cyberpolice.gov.ua/Офіційний сайт кіберполіції України

3. Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ. - //Економічна правда від 26 лютого, 2013року.

4. Комп'ютерна злочинність - К.: Атіка, 2002

Захищеність комунікаторів зв'язку від несанкціонованого доступу

Кохан О.В.
студентка кафедри захисту інформації Запорізького національного технічного університету
Куцак С.В.
науковий керівник, старший викладач кафедри захисту інформації Запорізького національного технічного університету

В наш час все гостріше відчувається необхідність в надійному захисті комунікаторів зв'язку від несанкціонованого доступу. Проблема безпеки інформації зростає з ростом кількості сфер комерційної діяльності, які використовують цифрові методи для передачі даних.