

КІБЕРЗЛОЧИННІСТЬ У ВСІХ ЇЇ ПРОЯВАХ: ВИДИ, НАСЛІДКИ ТА СПОСОБИ БОРОТЬБИ



У наші дні використання інформаційних технологій не має меж. Віртуальний простір переймає від реального все підряд, у тому числі й злочинність у її нових формах і проявах. Поняття кіберпростору, введеного письменником Вільямом Гібсоном у п'єсі «Le Neuromancer», описує віртуальний простір як такий, в якому циркулюють електронні дані всіх комп'ютерів світу.

Практично кожен чув про кіберзлочинність і, можливо, навіть особисто з нею зіштовхувався. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою комп'ютера і в мережі Інтернет. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні.



Піратство та кіберзлочинність в Україні

Нормативне регулювання цієї сфери в Україні не встигає за розвитком технологій, що загострює проблему кіберзлочинності. На рівні фізичних осіб кіберзлочинність пов'язана з використанням піратського програмного забезпечення: зловмисники можуть отримати доступ до персональних даних користувача. Згідно з дослідженням Асоціації виробників програмного забезпечення (BSA) за 2011, рівень піратства в Україні становив 84%. За оцінками Міжнародного альянсу інтелектуальної власності (IIPA), Україну визнано «піратом №1» у світі.

Піратство створює сприятливі умови для розвитку кіберзлочинності. За словами начальника кіберполіції України Сергій Демедюка, збитки від кіберзлочинів в Україні за перші 8 місяців 2016 року становлять близько 27 млн гривень. Для прикладу: в 2014 році наслідки кіберзлочинів коштували українцям 39 млн гривень.

В Україні до кіберзлочинів відносять порушення авторського права і суміжних прав, шахрайство, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення; ухилення від сплати податків, зборів (обов'язкових платежів), ввезення, виготовлення, збут і розповсюдження порнографічних предметів, незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю.

Кіберзлочини як загроза для кожного

Об'єктом кіберзлочинів може стати будь-який користувач інтернету.

Найпоширенішими видами таких злочинів є:

Кардинг - використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»).

Фішинг - вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі.

Вішинг - вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський 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 TV.

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.

Існує декілька порад щодо того, як вберегти себе від кіберзлочинів:

- ❖ створення надійних паролів, захист інформації та періодична їх зміна;
- ❖ поінформованість про розповсюджені прийоми, які використовують злочинці для того, щоб розпізнавати їх;
- ❖ захист пристроїв, встановлення антивірусних програм;
- ❖ використання захищених мереж;
- ❖ перевірка своїх облікових записів;
- ❖ використання інструментів конфіденційності та безпеки Google чи інших браузерів.

Кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам

Однак, за його словами, у 2016 році відбувся значний прогрес у цій сфері, зокрема на інституційно-організаційному рівні: у березні 2016 року уряд прийняв Стратегію кібербезпеки України, яка має на меті створення національної системи кібербезпеки;

у червні 2016 року Президент України підписав Указ про створення Національного координаційного центру кібербезпеки. Першим етапом його роботи є здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки;

у вересні 2016 року Верховна Рада у першому читанні прийняла закон про основні засади забезпечення кібербезпеки України.

Тож протидія кіберзлочинності та рівень кібербезпеки на сьогодні є одним із пріоритетних напрямків в політиці країни. Але для комплексної боротьби з цією проблемою потрібні спільні зусилля держави, громадян та міжнародної спільноти.