валідовані, щоб переконатися в їх надійності та ефективності.

Слід зазначити, що використання дронів також може мати етичні та правові наслідки, зокрема щодо порушення приватності та безпеки громадян. Крім того, дрони можуть стати об'єктом кібератак, що може призвести до витоку конфіденційної інформації або перехоплення керування дроном. У цілому, військові дрони мають великий потенціал у військових діях, проте їх використання повинно бути обмеженим та контрольованим з метою забезпечення безпеки та дотримання міжнародного права.

УДК004

В.О. Данилко , студентка гр.103ТН
Т.М. Деркач, к.т.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

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. Слід відмітити, що кіберзлочинці суттєво активізували діяльність у період воєнного стану в Україні.

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 останні роки напередодні війни рівень піратства в Україні становив більше 80%. За оцінками Міжнародного альянсу інтелектуальної власності (IIPA), Україну визнано «піратом №1» у світі.

Піратство створює сприятливі умови для розвитку кіберзлочинності. Збитки від кіберзлочинів в Україні з кожним роком зростають і вимірюються мілiонами 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.

Кіберзлочини як загроза державі

Питання кіберзлочинності є надзвичайно важливим на державному рівні. Найчастіше під ударами кібератак опиняються об’єкти критичної інфраструктури: енергетичні об’єкти, транспорт та банківський сектор. Вартість захисту зазвичай у 10 разів дорожча за саму атаку. Тому пріоритетним напрямком в політиці багатьох держав є кібербезпека.

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.

УДК004

О.Г. Чобітько , студентка гр.103ТН
Т.М. Деркач, к.т.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ОСНОВНІ НАПРЯМКИ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Розвиток інформаційних технологій є невід'ємною частиною сучасного світу. За останні десятиліття технології зазнали значного розвитку, що дозволило значно полегшити та прискорити багато процесів у різних сферах життя.

Однією з найбільш відчутних змін є зростання швидкості та доступності Інтернету. Це дозволило людям отримувати доступ до інформації з будь-якого місця та в будь-який час, а також забезпечило зручність та швидкість комунікації.

Також інформаційні технології знайшли своє застосування у бізнесі, науці, медицині, освіті та інших сферах. Вони дозволяють зберігати та обробляти великі обсяги даних, автоматизувати процеси та забезпечувати більш ефективну роботу.

Однак, разом з розвитком технологій з'являються нові виклики та проблеми, такі як кібербезпека, приватність даних та залежність від технологій. Тому важливо розуміти, що розвиток інформаційних