УДК 004.056.5

КІБЕРЗЛОЧИНИ

Седневець В.І., студ.гр.КБ-181,
Усов Я.Ю., викладач кафедри кібербезпеки та математичного моделювання
Чернігівський національний технологічний університет

Проблема кібербезпеки дуже актуальна в наш час . Щороку в світі відбувається величезна кількість кіберзлочинів . Тому дуже важливо щоб кожен знав все про кіберзлочини та як захистити себе і свої дані від кіберзлочинців.

Кіберзлочин - суспільно небезпечне винне діяння у кіберпросторі або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність або яке визнано злочином міжнародними договорами України.

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 .

До основних видів кіберзлочинів можна віднести : незаконний доступ; незаконне перехоплення; втручання у дані або у систему; зловживання пристроями; шахрайство, пов'язане із комп'ютерами; порушення авторських і суміжних прав; правопорушення, спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних .

Найбільш поширена класифікація кіберзлочинів в даний час ґрунтується на структурі Конвенції Ради Європи про кіберзлочинність. Ця класифікація в даний час виступає «еталоном», оскільки наявні міжнародні та регіональні документи, а також наукова практика, використовують саме цей поділ :

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:
   - незаконний доступ;
   - втручання в дані;
   - втручання в систему;
   - зловживання пристроями;
2) правопорушення, пов'язані з комп'ютерами;
3) правопорушення, пов'язані зі змістом;
4) правопорушення, пов'язані з порушенням авторських та суміжних прав .

Найпоширенішими кіберзлочинами є кібершахрайство , протиправний контент , фішинг , кардинг та поширення шкідливого програмного забезпечення . Під кібершахрайством розуміють викрадення персональних даних з банківських карт . Протиправний контент це поширення пропаганди тероризму , жорстокості та небезпека для інтелектуальної власності. Під час фішингу створюють веб-сайти схожі на оригінали та надсилають електронною поштою повідомлення з проханням вказати свої рахункові дані та паролі. Кардинг заключається в використанні в операціях реквізитів платіжних карт , отриманих із персональних комп'ютерів та зламаних серверів інтернет-магазинів , платіжних і розрахункових систем . Поширення шкідливого програмного забезпечення небезпечне викраденням персональних даних с комп'ютера або телефону , та продажем цієї інформації. Більшість людей скачують неліцензійне програмне забезпечення та цим ставлять під загрозу свої особисті дані .

Еволюція кіберзлочинів . З самого початку існувало багато різних каналів, через які хакери обмінювались інформацією, розробками , ділилися знаннями, інформацією, своїми чи піратськими програмами. Коли почала розповсюджуватися інтернет-торгівля , з'явилося багато форумів про те, як отримувати гроші через спам, фішинг, хакерські програми та веб-атаки. Наступний етап - це поява фальшивих антивірусних програм. Хакери встановлювали на комп'ютер жертви дуже погану антивірусну программу яка насправді жодних вірусів не виявляє. Програма виводить повідомлення про виявлення на комп'ютері багатьох проблем і необхідність придбання конкретної програми за гроші для того щоб позбутися тих проблем на комп'ютері. Згодом з'явився наступний клас хакерських програм: програми-блокувальники. Вони пробираються через браузер і запускають вікно на весь екран з текстом про те, що вас впіймали за переглядом переглядом протиправного контенту і вимагали гроші . Згодом виник новий клас подібних програм - програми, що вимагають, шантажують. Розвитку програм-вимагачів сприяє поширення віртуальної валюти Bitcoin, адже ця валюта майже не має тих обмежень, які є у кредитних карток чи інших платіжних систем. Також якщо раніше розробники хакерських програм самі розсилали спам, аналізували результати й обирали собі жертв , то зараз програмісти пишуть хакерські програми на продаж. Ви купуєте в них програму, в яку вшитий ваш ідентифікаційний номер, і поширюєте її. Коли хтось ловиться на гачок, автори програми знають, що це сталося за вашого посередництва і ви ділите прибуток - 70% вам і 30% їм.

Ось декілька найвідоміших кібератак :

Хакерське угрупування Fin7 складу якого входили і українці . Це група людей що працюють злагоджено та вкрали приблизно 15 млн. банківських номерів та мають прибуток приблизно 50 млн. доларів в місяць . Вони розробляли шкідливі програмні засоби , крали банківські номери із баз даних ресторанів та магазинів і використовували методику фішингу .

Вірус Petya який наробив галасу в 2017 році . Він вразив багато банків , державних та комерційних підприємств . Цей вірус блокує доступ до жорсткого диску , та виводить повідомлення про вимагання викупу для розшифрування файлів комп'ютера .

Вірус WannaCry атакували комерційні та урядові установи 12 травня 2017 року . Також цього нападу зазнав увесь світ. Цей вірус шифрує файли а потім виводить повідомлення про ціну за яку ці файли будуть розшифровані , але у випадку якщо ви не заплатите протягом 7 днів, вірус знищить файли.

Anonimus – це сучасна міжнародна спільнота активістів у яких немає лідера . Вони виступають проти цензури , переслідування і нагляду . В знак протесту вони зламали багато державних веб-сайтів та великі організації з безпеки . В 2012 році Anonimus провела найбільшу DDoS-атаку в історії з застосуванням LIOC. Під час цієї атаки було виведено з ладу сайти ФБР , Білого дому, Американського управління авторського права , Міністерства юстиції , Universal Music Group , Американської асоціації звукозаписних компаній, Американської асоціації кінокомпаній.

Комп'ютерний черв'як Stuxnet що виводить з ладу комп'ютери під управлінням операційної системи Microsoft Windows , у 2012 році вивів з ладу іранські центрифуги . Він фізично руйнує інфраструктуру та може використовуватись для шпіонажу та збирання даних.

BlackEnergy3 –троянська програма через яку було вимкнено близько30 підстанцій та близько 230 тисяч мешканців на 6 годин залишились без світла. Зараження системи відбувається через вразливі документи Microsoft Office . Атак в Україні зазнали : «Прикарпаттяобленерго» , «Чернівціобленерго» та «Київобленерго».

Угруповання Fancy Bear , що спеціалізуються на кібершпигунстві відоме атаками на інформаційні системи урядових , військових , безпекових організацій . Це угрупування відносять до типу розвиненої сталої загрози . Також це угрупування відоме як Pawn Storm , Sofacy Group , APT28 , Sednit. Воно створювало фальшиві сервери, підроблені під корпоративні сервери жертв з метою викрадення їхніх облікових даних .

Зрозуміло що ми не можемо захиститися від усіх кібератак , але кожен з нас може не дозволити собі стати жертвою кіберзлочину . Для цього потрібно слідувати таким порадам : не слід надавати комусь персональні дані, паролі і коди-підтвердження з смс для операцій з картками; не довіряти повідомленням про виграші в лотереях; перевіряти інформацію за офіційним номером банку; не скачувати в інтернеті сумнівні файли; користуватись ліцензійним програмним забезпеченням; не переходити через підозрілі посилання на інші сайти; користуватися антивірусними програмами та використовувати тільки захищені мережі; створювати надійні паролі та періодично їх змінювати і використовувати інструменти конфіденційності браузерів. Сумнівний номер телефону чи картки можна перевірити на сайті кіберполіції, а також звернутися до спеціалістів із запитом .

Отже , в наш час існує дуже багато загроз нашим даним . Нажаль не всі слідують тим правилам безпеки в інформаційному просторі і тим самим наражають себе на небезпеку . Дуже важливо розвивати наші знання у сфері кібербезпеки .

Список використаних джерел

1. Екскурсія за лаштунки кіберзлочинності [Електронний ресурс]. Режим доступу: https://www.bbc.com/ukrainian/features-39091289

2. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби [Електронний ресурс]. Режим доступу: https://www.gurt.org.ua/articles/34602/

Поняття та зміст кіберзлочинності [Електронний ресурс]. Режим доступу: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/

УДК 004.056.5

КРИТЕРІЇ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Коротка Г.М., студентка гр. КБ - 161

Усов Я.Ю., викладач кафедри кібербезпеки та математичного моделювання

Чернігівський національний технологічний університет

Сучасна людина занурена в інформаційне середовище, адже глобальний процес інформатизації суспільства охопив практично всі країни світу і нині є головним чинником науково-технічного і соціально-економічного розвитку. Інформаційне середовище – сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, а також соціально-економічних і культурних умов реалізації процесів інформатизації. У зв'язку впровадженням інформаційних систем у фінансові, юридичні, промислові, торгові й соціальні галузі швидко зріс інтерес до проблем збереження й захисту інформації.

Для запобігання загроз інформаційній безпеці створюються комплекси засобів захисту інформаційного середовища. Комплекс засобів захисту інформації — це сукупність програмно-апаратних