Презентація на тему Кібер злочинність

Зробив Ошейко Данііл
Учень 8-Б класу

Проблеми та актуальність

- Я вважаю що проблема кібер злочинності є актуальною у наш час . Особливо у

Види кібер злочинів

- *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.

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. Щоб дізнатися про стан рівня кібербезпеки в Україні, ГУРТ звернувся до **Дмитра Дубова, завідувача відділу інформаційної безпеки Національного інституту стратегічних досліджень**: «Уявлення України про кібербезпеку поки досить абстрактні, проте ведеться активна робота в цьому напрямку. Питанням кібербезпеки зараз займаються різні відомства: Державна служба спеціального зв'язку і захисту інформації, Служба безпеки України, Міністерство внутрішніх справ, Національний банк. Кожне з відомств вживає заходів щодо безпеки і веде статистику відповідних показників, проте їхня діяльність охоплює тільки окремі власні сфери відповідальності. Цілісна політика поки відсутня, як і універсальні індикатори кібербезпеки, що могли б охарактеризувати її рівень», – прокоментував **Дмитро Дубов.**

Кевин Митник

- Американец Кевин Митник — наверное, самый известный в мире хакер, во многом благодаря склонности к эксцентричному поведению, которого от него и ожидала праздная публика. Во время своего ареста в 1995 году Митник безапелляционно заявил, что ему достаточно посвистеть в трубку уличного телефона-автомата, чтобы развязать ядерную войну.
- В действительности, конечно, ничего подобного он сделать не мог, поскольку, пусть и действительно взломал множество защищённых сетей, но использовал для этого вовсе не какие-то гениальные программы и сверхъестественные коды, а банальные методы социальной инженерии — проще говоря, человеческий фактор. Митник применял не столько какие-то технические навыки, сколько знание психологии и манипулировал людьми, заставляя их выдавать свои пароли.
- Практиковаться во взломе различных систем Митник начал с детства. Известно, что в 12-летнем возрасте он нашёл способ подделки автобусных билетов, который позволял бесплатно перемещаться по всему городу. Затем он «перехватил» управление системой голосовой связи в местной закусочной «МакАвто», чтобы говорить посетителям всякие гадости.
- В шестнадцать лет Митник взломал сеть фирмы Digital Equipment Corporation и похитил размещённое там программное обеспечение: это стоило ему года в заключении и трёх лет под надзором полиции. Именно в это время он влез в систему голосовой почты Pacific Bell и после того, как был выписан ордер на его арест, пустился в бега.
- В 1999 году поймавшие Митника агенты ФБР утверждали, что при нём были фальшивые документы и мобильные телефоны с «клонированными» номерами. В итоге его обвинили во взломе нескольких компьютерных и телефонных сетей и приговорили к 46 месяцам заключения плюс 22 месяца за нарушение условий условного освобождения; при этом шутка про ядерную войну обошлась ему в восемь месяцев в «одиночке».
- Кевин Митник вышел из тюрьмы в 2003 году и с тех пор написал несколько книг о своих хакерских достижениях. В 2000-м вышел фильм «Взлом» (Track Down) на основе его биографии, написанной Цутому Симомурой и Джоном Маркоффом, причём Симомура был экспертом по компьютерным системам, чей компьютер был взломан Митником. Сегодня Митнику 49 лет, и он управляет собственной компанией по компьютерной безопасности.