та політичних лідерів більшості країн на пропозиції щодо глобальної боротьби з тероризмом».

Здійснювати кібертеракти сьогодні здатна будь-яка з існуючих в даний час терористичних організацій - Ірландська організація ІРА, «Аль-Каїда», баскська організація ЕТА, релігійні рухи типу алжирських або єгипетських фунд аменталістов, чеченські незаконні збройні формування і т.п. Наразі, на прикладі комп'ютерного хробака Стакснет (win32/Stuxnet), що вражає комп'ютери, які працюють на операційній системі Microsoft Windows. Це перший відомий комп'ютерний хробак, що перехоплює і модифікує інформаційний потік між програмованими логічними контролерами марки SIMATIC S7 і робочими станціями SCADA-системи SIMATIC WinCC фірми Siemens. Таким чином, хробак може бути використаний як засіб несанкціонованого збору даних (шпигунства) і диверсій у АСУ ТП промислових підприємств, електростанцій, аеропортів тощо. Важливо зрозуміти, що якщо такий хробак зроблять терористи вони будуть в силах зробити майже будь-яку диверсію або атаку на існуючий комп'ютер.

Міжнародна інформаційна безпека обумовлюється стратегічною спрямованістю інформаційних озброєнь проти найважливіших структур життєдіяльності і функціонування людства, визнання інформаційної зброї як нового глобального виду зброї масового ураження, катастрофічного за наслідками свого застосування, необхідністю створення міжнародного механізму протидії і попередження глобальних інформаційних війн в рамках політичної компетенції ООН, регіональних міжнародних організацій з проблем безпеки та оборони, політичних рішень на національному рівні. Таким чином, проблема кібертероризму є вагомою складовою загальних проблем у сфері інформаційної безпеки і проявом тенденцій нових глобальних викликів і глибинних процесів глобалізації комунікацій.

Список використаних джерел:

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [Електронний ресурс] – Режим доступу : http://zakon.rada.gov.ua

2. Міжнародна інформаційна безпека: Сучасні виклики та загрози [Текст]. – К.: Центр вільної преси, 2006. – 916 с.

3. Юдін О.К. Інформаційна безпека держави: Навчальний посібник [Текст] / О.К. Юдін, В.М. Богуш. – Х.: Консум, 2005. – 576 с.

Махницький О.В.
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровський державний

університет внутрішніх справ

КЛАСИФІКАЦІЯ КІБЕРЗЛОЧИНІВ

Прискорений розвиток суспільства, його прагнення до скасування кордонів, інтеграції та глобалізації тягнуть за собою різні наслідки, на жаль, не завжди позитивні. Досягнення науки і техніки, створення всесвітньої мережі Інтернет дозволили злочинності вийти на новий рівень і захопити кіберпростір.

Тепер злочинцеві не потрібен прямий контакт з жертвою і лише кілька людей можуть стати загрозою для кожного користувача «глобальної павутини», великих корпорацій і цілих держав.

Інформаційні технології в глобальному сенсі - це спільний доступ до зберігання та обробки інформації. Сучасне суспільство орієнтоване на величезну кількість інформації, яка доступна і змінюється щохвилини. Фахівці в галузі кримінального правосуддя покладаються на цю інформацію, щоб розслідувати кібер-злочину. Кожен день приносить нові можливості для технологічних досягнень, які можуть допомогти фахівцям у проведенні кримінальних розслідувань. На жаль, ці технологічні досягнення створюють можливості для злочинців у скоєнні злочинів з використанням тієї ж технології, що є частиною повсякденного життя для більшості людей. Фахівцям в галузі кримінального правосуддя необхідно бути завжди в тренді і мати широке розуміння технологій і напрямки їх розвитку. Вони також повинні бути готові до адаптації і розширення їх знань інформаційних технологій для того, щоб залишатися на крок попереду злочинців.

Кібер злочин - це будь-який злочин в електронній сфері, вчинений за допомогою комп'ютерної системи або мережі, або проти них.

Поширені типи кібер злочинів.

Сучасні технології практично невіддільні від нашого повсякденного життя. Проте, злочинці часто використовують уразливості в системі безпеки для вчинення злочинів шляхом використання комп'ютерної техніки. Якщо представники громадськості не обізнані про комп'ютерну безпеку, вони можуть легко стати жертвою інтернет-шахраїв. Нижче наведені найпоширеніші види кібер злочинів

Шахрайство в соціальних мережах.

Шахраї реєструються в соціальних мережах з логінами або адресами електронної пошти та паролями, придбаними незаконним шляхом. Потім вони заходять на сторінки зі списку контактів в якості справжніх користувачів цих акаунтів і вводять в оману пропонуючи купити неіснуючий товар з передоплатою або з проханням допомогти матеріально в зв'язку з несподіваними обставинами. Вони також можуть попросити коди авторизації або паролі від пластикових карт. Після отримання такої інформації зловмисник як правило видаляє аккаунт і знайти його вкрай складно.

Електронний банкінг.

Дуже поширений вид шахрайства, що полягає в тому, що зловмисник надсилає потенційній жертві електронного листа підозрілого змісту, що

спонукає жертву відкрити вкладення. В наслідок чого комп'ютер жертви заражається шкідливою програмою, яка щороку збирає персональну інформацію і відправляє її зловмисникові.

Спам в електронній пошті.

В даний час електронна пошта є найпоширенішим каналом зв'язку між родичами, друзями і комерційними партнерами. Шахраї намагаються обдурити жертв усіма можливими засобами, щоб змусити їх зробити грошовий переказ. Найчастіше це неіснуючі благодійні фонди і волонтерські організації.

Соціальні мережі, спільноти-пастки.

Комп'ютерні та інформаційні технології принесли зручність для спільноти, дозволяючи людям з усіх верств суспільства і різних вікових груп отримувати інформацію з Інтернету і більш тісно взаємодіяти з друзями і родичами.

У той же час користувачами мережі все частіше стають діти і підлітки, які заводять нові знайомства з невідомими, знаючи їх тільки по сторінці в соціальних мережах.

Відповідно юні користувачі соціальних мереж, котрі вступають в різні спільноти не можуть знати достовірно, які цілі переслідує творець цієї групи, і до чого призведе тривале спілкування на даній сторінці. До вкрай негативних наслідків можна віднести спілкування підлітків в так званих «групах смерті».

Кібер злочину, пов'язані з онлайн-іграми.

Кібер злочини пов'язані з онлайн-іграми відносяться до таких кримінальних правопорушень як шахрайство. Покупець або Продавець не отримує будь-яких товарів або платежів після того, як оплата була проведена або товар був доставлений на інтернет-платформу.

Неправомірний доступ до комп'ютерної системи.

Злочин передбачає неправомірний доступ до комп'ютерної інформації, якщо це діяння спричинило знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі в цілому [2].

Інші види кібер злочинів.

Будь-яке інше правопорушення, в електронній сфері, вчинене за допомогою комп'ютерної системи або мережі, або проти них вважається кібер злочином.

Органи влади та представники комерційних фінансових установ регулярно звертаються до громадськості із закликами бути пильними і тим самим уникнути потенційних небезпек кібер злочинів.

Список використаних джерел:

1. On-line журнал «Правознавець» http://pravoved.in.ua/section-kodeks/134-yku/1147-031.html

Мирошниченко В.О.