КІБЕРАТАКИ – ТЕРОРИЗМ XXI СТОЛІТТЯ

Праховнік Н. А., доц., к.т.н., (каф. ОПЦБ КПІ ім. Ігоря Сікорського);
Землянська О.В., ст. викл. (каф. ОПЦБ КПІ ім. Ігоря Сікорського);
Максим К. Є., студ. (гр. КВ-73мп, ФПМ КПІ ім. Ігоря Сікорського)

Анотація. У статті досліджені питання, пов'язані із визначенням поняття кібертероризм, а також здійснено спробу опису принципів захисту від кібератаки в сучасних умовах.

Ключові слова: кібертероризм, інформаційні технології, безпека.

Annotation. The article studies the issues related to the definition of cyberterrorism, and an attempt is made to describe the principles of protection against cyber attacks in modern conditions.

Keywords: cyberterrorism, information technology, safety.

Постановка проблеми. У XXI столітті кібератаки стають все більш відчутною, потужною загрозою для безпеки не тільки окремих користувачів, підприємств або Інтернет-ресурсів, а й держав. Вони можуть вивести з ладу окремі об'єкти інфраструктури, дестабілізувати роботу цілих систем.

За даними різних аналітичних структур загальні світові витрати, пов'язані з кіберзлочинністю, перевищують комбінований вплив на всесвітню економіку від торгівлі наркотиками. Кожну секунду десяток осіб стають жертвами кібер-шахрайства. Причому найбільш ймовірними жертвами стають молоді люди, які виходять в Інтернет через мобільні телефони.

Злочини у сфері інформаційних технологій дуже часто є міжнародними, тобто злочинці діють в одній державі, а їх жертви знаходяться в іншій. Тому для боротьби з такими злочинами особливе значення має міжнародне співробітництво. Все більше розвинених країн прагнуть захиститися шляхом створення спеціальних підрозділів, що діють у складі спецслужб.

Аналіз останніх досліджень. Кібертероризм став центральним об'єктом наукових досліджень Б.Коліна, старшого наукового співробітника американського Інституту безпеки і Розвідки.

Мета і завдання дослідження. Мета даного дослідження полягає у визначенні такого поняття як кібертероризм та опису принципів захисту від кібератаки у сучасних умовах.

Виклад основного матеріалу дослідження

У минулому році Україна стала абсолютним лідером за внутрішніми та зовнішніми кіберзагрозами в Європі. І це не дивно – за останні роки наша країна неодноразово ставала мішенню не тільки для дрібних шахраїв, а й для масштабних кібероперацій.

Відповідно до нині прийнятих формулювань кіберзлочинність це злочини в сфері інформаційних технологій, що здійснюються людьми з використанням даних технологій для злочинних цілей.

Одним з найбільш небезпечних і поширених злочинів, скоєних з використанням Інтернету, є шахрайство в усіх його видах, включаючи крадіжку

даних фінансових структур. Іншим найбільш згубним діянням кіберзлочинності може вважатися поширення в мережі різного роду вірусів, як з метою крадіжки інформації, так і просто руйнування будь-яких структур і систем. Вживаючи термін «кібертероризм» розуміють дії по зловмисному проникненню в інформаційні системи, за рахунок чого створюється небезпека загибелі людей, значної майнової шкоди чи інших суспільно небезпечних наслідків.

Таким чином, можна вважати, що кібертероризм є не що інше, як певний різновид тероризму, спрямований на залякування і інший вплив на прийняття рішень різних структур з використанням сучасних інформаційно-телекомунікаційних технологій.

Жертвами сучасних вірусів стають не тільки рядові користувачі і їх файли. У травні 2016 року під час атаки вірусу WannaCry змушені були припинити свою роботу близько 40 медичних закладів Британії так як їх комп'ютерне обладнання було пошкоджено шкідливим програмним забезпеченням. У постраждалих від атаки мед установах був зупинений прийом амбулаторних хворих, порушена робота «швидкої допомоги» і навіть виник збій в проведенні запланованих хірургічних операцій.

В цьому році хакерська атака вірусом Petya.A інфікувала 12,5 тисяч українських комп'ютерів, тим самим зупинивши роботу десятків українських банків, медіа ресурсів, сайтів державних установ, мобільних операторів та компаній перевізників. Економічні витрати від атаки вірусу Petya.A можуть перевищувати $ 8 млрд., такий висновок зробила компанія Cyence, що займається оцінкою ризиків. У цей перелік компанія підрахувала ще й шкоду, заподіяну травневою атакою схожого вірусу WannaCry, який призвів до виходу з ладу понад 200 тисяч комп'ютерів у 150 країнах світу. Кібератака вірусу Petya стала шоком для фінансової системи. Повністю замороженим виявився фондовий ринок, частково були паралізовані банківська система і страховий ринок. І все це відбулося в кінці фінансового кварталу.

Слід зауважити, що порушення правил кібербезпеки не в перший раз ставить під загрозу роботу стратегічно важливих об'єктів інфраструктури в Україні. Вірус Petya – вже третя за рахунком кібератака в Україні за останні два роки, хоч і перша настільки масштабна. І може стати не останньою. Так, в грудні 2016 року хакерській атаці піддалися установи Мінфіну, комерційні банки, об'єкти «Укренерго» та інфраструктури. Через це Київ на декілька годин залишився без електроенергії.

Очевидно, що українським компаніям, в першу чергу державним, варто серйозніше поставитися до інформаційної безпеки. В ході усунення наслідків від кібератаки розкрилася проблема практично повної відсутності кваліфікованих фахівців, які могли б забезпечити належне реагування на інцидент. Навіть компанії, що мають великий штат IT-фахівців неспроможні були організувати якісну реакцію на інцидент і локалізувати наслідки атаки.

Причин для цього кілька. Оскільки атаки тривають і видозмінюються то частина рекомендацій щодо захисту стають неактуальними. А також, однією з основних проблем є недостатній досвід IT-фахівців в реагуванні на атаки.

У сучасних реаліях комплекс заходів щодо подальшого реагування на подібні ситуації потрібен не менше, ніж інструкції щодо дій при виникненні надзвичайних ситуацій. Необхідно відзначити, що на поточний момент захиститися від шкідливих програмних продуктів на 100% неможливо.

Під захистом від кібератак розуміють методи мінімізації шляхів через які зловмисники можуть проникнути і розповсюдити шкідливе програмне забезпечення в IT-інфраструктурі організації. Одним з основних напрямів боротьби є створення максимально «несприятливих» умов для зловмисників, для того, щоб виявити присутність хакерів в інфраструктурі жертви можна було б на будь-якому з етапів інтерактивної взаємодії зловмисника з програмним забезпеченням організації.

Всі ці методи реалізовуються за допомогою комплексного захисту. Це технічні засоби, а також перевірені і затверджені процеси взаємодії підрозділів інформаційних технологій та інформаційної безпеки. До технологій можна віднести такі продукти, як:

- SIEM (системи управління інформаційною безпекою);
- фаєрвол, IDS/IPS (системи безпеки периметра і сегментації мереж);
- DLP (системи запобігання витоку конфіденційної інформації);
- VPN (створення зашифрованих каналів зв’язку);
- OTP (генерація одноразових паролів);
- антивіруси (стандартний антивірусний захист);
- patching (процес управління установкою оновлень ПО);
- бекапи (зберігання резервних копій системи);
- awareness (процес навчання користувачів по інформаційній безпеці);
- pentest (незалежний аналіз захищеності) і т.п.

Варто зазначити, що задля досягнення оптимальної безпеки від кібератак необхідно оцінювати ризики та постійно підтримувати процеси безпеки у поєднанні з одноразовими рішеннями та усуненням вразливих місць.

Висновок

Аналіз практики протидії кіберзлочинності та кібертероризму в Україні і за кордоном, зростаюча ступінь суспільної небезпеки висувають завдання оптимізації заходів щодо вдосконалення законодавчого забезпечення протидії існуючим і прогнозованим загрозам у цій сфері, а також наголошують на потребі в кваліфікованих IT-фахівцях.

Література

1. Климентьев К., Компьютерные вирусы и антивирусы. Взгляд программиста. Москва: ДМК Пресс, 2013, 29с.

2. https://uk.wikipedia.org/wiki/Інформаційна_безпека.

3. Князев А. А. Информационная война // Энциклопедический словарь СМИ. – Бишкек: Издательство КРСУ, 2002.