МІНІСТЕРСТВО АГРАРНОЇ ПОЛІТИКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

Факультет економіки і підприємництва

Кафедра

Доповідь

з дисципліни "Автоматизоване робоче місце бухгалтера "

на тему:

«Кібервійни»

Виконала:
студентка групи 43-ОА
Яременко Віта Віталіївна

Керівник:
Гиренко Ю. В.

В сучасному світі, в якому дедалі більшу роль в житті держави, її економіці та системі безпеки, відіграють кіберпростір та сучасні інформаційні технології, не можна обійти увагою ті загрози, які пов’язані з застосуванням цих високих технологій. У цьому зв’язку все частіше можна почути такі слова, як «кібершпигунство» та «кібервійна».

В сучасній літературі саме поняття «кібервійна» є багатозначним. Так, наприклад, електронна енциклопедія «Вікіпедія» визначає кібервійну так: «кібервійна є використанням комп’ютерів та Інтернету при проведенні війни у кіберпросторі». Цілком ясно, що така дефініція є занадто широкою і може охоплювати різні недостатньо серйозні прояви хакерства та «віртуального хуліганства».

На нашу думку, кібервійну точніше було б визначити як застосування комп’ютерних технологій та Інтернету однією державою, або за її безпосередньої підтримки, проти іншої держави, спрямоване проте її безпеки і оборони, яке є настільки інтенсивним і серйозним, що становить реальну загрозу безпеці та суверенітету цієї іншої держави.

Спеціалісти виділяють такі види атак в інтернеті:

- Вандалізм — використання хакерами інтернету для паплюження інтернет сторінок, заміни змісту образливими чи пропагандистськими зображеннями.
- Пропаганда — розсилка звернень пропагандистського характеру, або вставка пропаганди в зміст інших інтернет сторінок.
- Збір інформації — зламування приватних сторінок чи серверів для збору секретної інформації чи її заміни на фальшиву, корисну іншій державі.
- Відмова сервісу — атаки з різних комп'ютерів для унеможливлення функціонування сайтів чи комп'ютерних систем.

- Втручання в роботу обладнання — атаки на комп'ютери, які займаються контролем над роботою цивільного чи військового обладнання, що призводить до його відключення чи поламки.
- Атаки на пункти інфраструктури — атаки на комп'ютери, які забезпечують життєдіяльність міст, їх інфраструктури, таких як телефонні системи, водопостачання, електроенергії, пожежної охорони, транспорту, тощо.

З поширенням комп'ютерних технологій та інтернету багато громадян, підприємств і державних установ почали залежати від інтернетного зв'язку у повсякденному житті. Використання інтернету для атак комп'ютерних систем іншої держави може завдати значної шкоди її економіці і створити розлад у повсякденному житті країни. На відміну від кібер-атак минулого зараз кібервійна являє собою загрозу для національної безпеки країн і сприймається багатьма як серйозна загроза безпеці держави.

Крім того, розвідувальні організації багатьох країн займаються шпигунством використовуючи інтернет: збирають інформацію, зламують комп'ютерні системи інших держав, займаються диверсійною діяльністю та економічним шпигунством. За визнанням спеціалістів, лідерами у веденні кібервійни зараз є Китай та Росія. Зокрема Китай звинувачували у організації атак на сайти Сполучених Штатів, Німеччини, Індії. Росія використовує інтернет не тільки для збору інформації, але й для організації масованих атак на недружні країни. Так після подій навколо Бронзового солдата, Естонія зазнала однієї з наймасовіших атак на державні установи і підприємства, що призвело до значного розладу в нормальному житті країни. Росія, як і Китай, однак заперечують причетність державних установ до організації атак.

Беруть участь у кібервійнах і українські хакери. Так після подій навколо акту вандалізму на Говерлі, сайти Євразійського союзу молоді, який взяв відповідальність за їхнє проведення, були атаковані з України. У відповідь зазнали атак сайти президента України та СБУ. Мабуть,

найяскравішим прикладом кібершпигунства є масштабна кібершпигунська операція, яка отримала назву GhostNet. Ця операція, в організації якої підозрюють уряд Китаю, охопила 1 295 комп'ютерів на цілому світі, третина яких знаходилась у міністерствах закордонних справ, посольствах, міжнародних організаціях та великих приватних фірмах. На думку канадських експертів, серед цих комп'ютерів був також комп'ютер зі штаб-квартири НАТО в Брюселі.

За даними зарубіжних аналітиків, щотижня у світі реєструється більше 55 млн комп'ютерних взломів – підраховані як результативні, так і безуспішні атаки хакерів. Більшість кіберзлочінців, до речі, базуються в азіатських странах. Ущерб, завданий йому користувачами Всесвітньої павутини в результаті хакерську нападів, в 2008 р., приміром, склав $ 14 млрд, і ця цифра збільшується з кожним роком.

Комп'ютерні зломи в даний час – аж ніяк не тільки прерогатива шахраїв-одинаків. "Аль-Каїда ", за інформацією ФБР, активно "заробляє" на злом кредиток жителів багатьох країн світу, а керівництво Естонії, мабуть, до цих пір шукає російський слід в хакерську атаку, що послідували відразу за знесенням "Бронзового солдата ".

Російські експерти з "Лабораторії Касперського" теж далекі від оптимізму. За даними аналітиків, у минулому році було зареєстровано найбільшу кількість комп'ютерних вірусів за всю історію. У річному аналітичному звіті компанії наголошується: "Це вселяє серйозні побоювання – адже якщо ситуація в 2009 р. не зміниться (а передумов для цього немає), то через рік нас чекає подвоєння кількості загроз ". Відзначимо, що минулого року компанія додала у свої антивірусні бази майже скільки ж програм, скільки за попередні 15 років. Вірусні аналітики підкреслили, що головним інструментом і "політизованих " і "кримінальних " хакерів залишаються DoS-атаки, що ведуть до обвалення серверів. Від цього виду зброї хакерів поки досить складно захиститися. Що ж до горезвісного спаму, то, за інформацією "Лабораторії Касперського", в 2009 р. його частка в поштовому трафіку

склала близько 79,2%. При цьому обсяг розсилки спаму протягом року зріс приблизно в два рази. Перше місце за кількістю рекламних розсилок займають США, далі йдуть Росія та Польща.

Шокуюче виглядають і результати аналізу Інтернету експертами IBM: тільки за перші шість місяців минулого року було виявлено більше трьох тисяч вразливостей в найбільш популярних комп'ютерних програмах, а на половині сайтів Мережі міститься контент, здатний інфікувати комп'ютери відвідувачів цих сторінок або замаскувати хакерську атаку.

Керівник дослідницького відділу фінської компанії «F-Secure» Мікко Гіппонен займається проблемами кібербезпеки вже майже 20 років: «В інтернеті небезпека чигає і на звичайних користувачів. Достатньо лише відвідати якусь сторінку в мережі – і відразу, навіть цього не помітивши, підхопити комп'ютерний вірус-троянець».

Мікко Гіппонен попереджає: «З цього моменту комп'ютер перестає бути твоїм. Його контролюють інтернет-злочинці, які хочуть заробити гроші. Вони або використовують твій комп'ютер для незаконних дій, приміром, розсилають з нього спам, або ж спостерігають, що відбувається з клавіатурою, сподіваючись, що ти робитимеш покупки в інтернеті й введеш номер своєї кредитної картки».

Передусім, інтернет стає найважливішим засобом для шпигунства - у промисловості, в політиці, у військових структурах: «Троянців усе частіше застосовують для шпигунства. Це відбувається постійно. І ми маємо достатньо підстав підозрювати, що за деякими такими нападами стоять окремі держави», - розповідає Гіппонен.

Наприклад, улітку 2007 року видання «Der Spiegel» повідомляло про появу вірусів-троянців у комп'ютерах німецького уряду. Припускалося, що сліди ведуть до Китаю. У вересні того ж року англійська газета «Times» писала про звіт Пентагону, згідно з яким китайські хакери розробили детальний план для Народно-визвольної армії Китаю з наміром паралізувати

кібератакою американський військовий флот. Крім того, вони розробили віртуальні інструкції ведення війни в кіберпросторі. Нинішній президент США Барак Обама надає цій проблемі великого значення, адже під час його власної передвиборчої кампанії минулого року хакери зламали комп'ютерну систему його виборчого центру. Наприкінці травня 2009 року Обама назвав безпеку комп'ютерних мереж одним з головних національних пріоритетів США. За оцінками експертів, уряд Сполучених Штатів щорічно витрачає на це 10 мільярдів доларів.

Касперський пророкує глобальні кібервійни в майбутньому: «Масштабні хакерські атаки можуть призвести до того, що відключеними від Мережі виявляться цілі країни, - вважає Євген Касперський. - У найближчому майбутньому нас очікують серії атак, націлені на знищення інтернет-інфраструктури держав». Деякі атаки здійснюють окремі хакери, але підтримку їм надають уряди - в цьому Касперський "упевнений на 90%". "Глобальна економіка залежить від Інтернету. Якщо у нас виникнуть серйозні проблеми з інтернет-інфраструктурою, якщо Інтернет буде відключений, ви забудете про фінансову кризу і глобальне потепління", - обіцяє він.

Як приклад голова "Лабораторії Касперського" привів Південну Корею і Естонію, яким вже довелося відбивати масовані атаки зловмисників.

Порятунок від хакерів Касперський бачить в об'єднанні всіх країн перед обличчям загрози. Раніше російський програміст вже закликав створити міжнародну організацію, яка б відслідковувала поширення в Мережі шкідливого ПЗ.

Оскільки світова економіка також дедалі більше залежить від Інтернету, зловживання інформаційними технологіями може серйозно зашкодити стабільності цієї економіки. З метою боротьби з такими загрозами деякі держави – члени НАТО (насамперед, США та Німеччина) вже створили спеціальний центр, який займається питаннями «кібербезпеки».

Виходячи з такої дефініції, кібервійну слід оголосити міжнародним злочином і розробити відповідну міжнародну конвенцію, спрямовану на попередження і боротьбу з проявами кібервійни.

На разі ми є свідками того, що деякі держави почали будувати національні системи кібербезпеки. Так, Сенат США розглядає можливість ухвалення відповідного закону, на базі якого буде створено інститут національного радника у справах кібербезпеки, котрий буде займатися цими питаннями в рамках Національного Агентства Безпеки (NSA), повітряних силах, Департаменті Національної Безпеки (DHS), а також в інших державних структурах. Відповідний закон передбачає вельми широкі повноваження для цього радника, у тому числі дає йому право виключати федеральні мережі у випадку «серйозної загрози». Якщо цей закон буде ухвалено, тоді може відбутися своєрідна мілітаризація кіберпростіру. Слід також пригадати, що на сьогодні майже всі американські концерни, які продукують зброю (наприклад, Boeing та Lockheed Martin) не тільки мають структурні відділи, які займаються забезпеченням кібербезпеки, але й також отримують солідну фінансову підтримку від уряду на розвиток кібербезпеки. Витрати американського уряду на створення безпечних комп'ютерних мереж мають вирости з 7,4 міліардів доларів США у 2008 році до 10,7 міліардів у 2013 році. Як передбачається, більшість країн НАТО підуть за прикладом США.

Цікаво, що в деяких країнах НАТО, наприклад в Естонії, порушено питання про необхідність впровадження спеціальних предметів з кібербезпеки навіть у школі.

Отже, кібербезпека все більше стає реальністю на національному рівні. Проте створення по-справжньому ефективної системи кібербезпеки не можна уявити без відповідних дій на міжнародному, світовому рівні. Саме тут особливу роль має відіграти міжнародне право і міжнародні структури, насамперед ООН. Першим кроком у цьому напрямі могло б бути скликання

спеціальної міжнародної конференції під егідою ООН, присвяченої міжнародно-правовим питанням кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-warfare/article/115929/>
2. Cyber-warfare // <http://en.wikipedia.org/wiki/Cyber-warfare>.
3. **Morozow J. Wrog z sieci // Newsweek, 24.05.2009. – S. 40–41.**
4. **www.securitylab.ru**
5. **Мерешко О. Проблеми кібервійни та кібербезпеки в міжнародному праві. // Юридичний журнал. – 2009. - № 6. – С. 94.**
6. **Наука і техніка від 18.06.2009 // Кібервійни – загрози 21 століття.**