УДК 004.7

Л.Ю. Крестьянполь
Луцький національний технічний університет

АНАЛІЗ СПОСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ НЕСАНКЦІОНОВАНОМУ ДОСТУПІ З ІНТЕРНЕТУ В ЛОКАЛЬНУ МЕРЕЖУ

Стаття присвячена аналізу потенційних загроз, що можуть виникнути при користуванні глобальною мережею Інтернет. Розглянуто організацію системи захисту інформації в сучасних інформаційних технологіях, виділено групи атак за певною ціллю та виконано огляд сучасних методів захисту даних в локальних мережах.
Ключові слова: *захист інформації, атаки, засоби захисту, локальна мережа.*

Л.Ю. Крестьянполь

АНАЛИЗ СПОСОБОВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ НЕСАНКЦИОНИРОВАННОМ ДОСТУПЕ ИЗ ИНТЕРНЕТА В ЛОКАЛЬНУЮ СЕТЬ

Статья посвящена анализу потенциальных угроз, которые могут возникнуть при использовании глобальной сети Интернет. Рассмотрена организация системы защиты информации в современных информационных технологиях, выделены группы атак по определенной цели и выполнен обзор современных методов защиты данных в локальных сетях.
Ключевые слова: *защита информации, атаки, средства защиты, локальная сеть.*

L. Krestyanpol

ANALYSIS OF INFORMATION PROTECTION METHODS IN CASE OF UNAUTHORIZED ACCESS FROM THE “INTERNET” IN THE LAN (LOCAL AREA NETWORK)

The article is devoted to the analysis of potential threats that may arise when using the “Internet”. The organization of the information security system in modern information technologies is considered. We identified attack groups for a specific purpose and reviewed current methods of protecting data in local networks.
Keywords*: information security, attacks, protection methods, local area network.*

Постановка проблеми. Сучасний розвиток технологій Internet призводить до необхідності захисту інформації, переданої в рамках локальної мережі від порушення інформаційних каналів і ресурсів; несанкціонованого доступу до інформації, що приводить до порушення її цілісності; руйнування засобів захисту що вбудовані, протиправних дій користувачів і обслуговуючого персоналу; впровадження “вірусів” і “закладок” в програмні продукти та технічні засоби. Для протидії атак та забезпечення надійної побудови системи захисту виділяють певну сукупність організаційно-технічних заходів і правових норм.

У статті здійснено огляд видів загроз інформаційної безпеки та наведено способи протидії при несанкціонованих доступах.

Аналіз останніх досліджень. Проблематикою захисту комп’ютерної інформації в свій час займались Б.Анин[1], А.В. Галицкий [2], дослідженням атак та загроз в локальних мережах - А. Лукацкий [3]. Детальним дослідженням атак через Інтернет займались И.Д. Медведовский, П.В.Семьянов, В.В. Платонов[4].

В свою чергу К. Касперский [5] описує техніку мережевих атак та займається створенням методів протидії при несанкціонованих доступах.

Виклад основного матеріалу. Поняття “інформаційної безпеки” є комплексним та включає у себе ряд наступних процедур, виконання яких в повній мірі забезпечить належний рівень захисту. До даних процедур відноситься: надійність збереження даних і програмного забезпечення, захист даних від несанкціонованого доступу, захист від крадіжки інформації, захист програмного забезпечення і апаратного забезпечення, захист від вірусів, збереження таємниці листування. Для виконання вище виділених процедур використовують різні заходи з захисту інформації

Захист інформації - це сукупність організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації. Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виключне право тієї або іншої держави. Проте в останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів із різноманітних країн.

На рисунку 1 наведено додатки які у 2015 році були використані зловмисниками для використання нових технік маскування експлойтів, шеллкодів і корисного навантаження з метою затруднення виявлення зараження і аналізу шкідливого коду [6].

Також, в таблиці 1 наведено ТОП – 10 країн з найбільшим процентом атак протягом 2015 року.

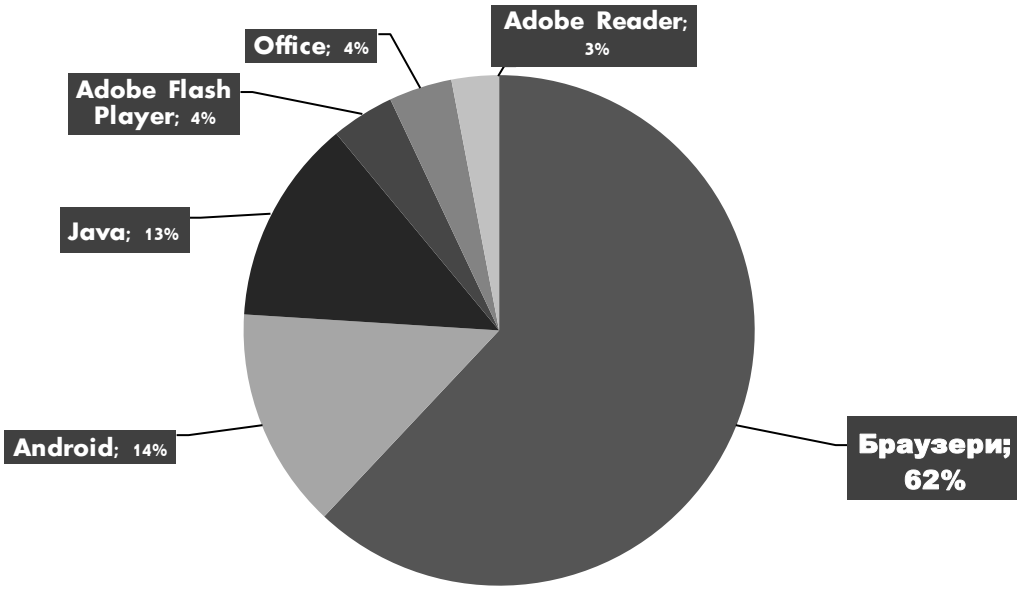

Рис. 1. **Розподіл експлойтів, використаних в атаках зловмисників, за типами атакованих додатків, 2015 рік**

Таблиця 1.

Перелік країн з найбільшим відсотком атак у фінансовій сфер серед користувачів Інтернет

№ п/п	Країна	Відсоток атакованих користувачів (%)
1	Сінгапур	11,6
2	Австрія	10,6
3	Швейцарія	10,6
4	Австралія	10,1
5	Нова Зеландія	10,0
6	Бразилія	9,8
7	Намібія	9,3
8	Гонконг	9,0
9	Південна Африканська Республіка	8,2
10	Ліван	6,6

В основному атаки здійснювались у фінансовій сфері за допомогою шкідливого програмного забезпечення, що використовується для атак на користувачів онлайн-банкінгу.

Що ж стосується України, то за даними Всесвітнього економічного форуму, відповідно до доповіді "Глобальний звіт про розвиток інформаційних технологій 2013: "Зростання та праця у гіперзв'язаному світі"", рейтинг України за основними індексами, що стосуються інформаційно-комунікаційних технологій щорічно зростає.

1. Індекс мережевої готовності (WEF Networked Readiness Index) 2013 рік – 73 місце, 2011–2012 роках — 75 місце із 142 країн (90 місце у 2010–2011 роках із 138 країн) [7];

2. Індекс технологічної готовності (WEF Technological Readiness Index) у 2012–2013 роках — 81 місце із 144 країн, у 2011–2012 роках — 82 місце із 142 країн та у 2010–2011 роках — 83 місце із 139 країн [8];

Хоча Україна все ще залишається на найнижчому рівні серед середньо-розвинутих каїн, встеж таки, тенденція росту дає підгрунття для початку аналізу та роботи у сфері захисту інформації в Інтернеті.

Організація системи захисту інформації в сучасних інформаційних технологіях

При побудові системи захисту, перш за все визначають можливі загрози для інформаційних ресурсів. Виходячи від роду загроз забезпечення інформаційної безпеки базується на комплексному підході.

Підгрунттям для реалізації політики захисту інформації є законодавчі акти. В організаційній структурі системи захисту інформації назвемо їх **"законодавчі засоби захисту"**. Вони визначаються законодавчими актами країни, в якій регламентуються правила використання, опрацювання і передачі інформації обмеженого доступу і встановлюються міри відповідальності за порушення цих правил.

Контроль за дотриманням вимог до захисту інформації та експлуатації спеціальних програмно-технічних засобів захисту, а також забезпечення організаційних заходів з захисту інформаційних систем, що опрацьовують інформацію з обмеженим доступом в недержавних структурах, здійснюються органами державної влади. Організації, які опрацьовують інформацію з обмеженим доступом, що є власністю держави, створюють спеціальні служби для забезпечення захисту інформації.

Ризик, пов'язаний з використанням не сертифікованих інформаційних систем лежить на власнику цих систем, а ризик, пов'язаний з використанням інформації, отриманих з сертифікованих систем, лежить на споживачеві інформації.

Наступним етапом побудови системи захисту є накази, розпорядження та інші дії керівництва організацій, пов'язаних з інформаційними системами, що захищаються.

Організаційні засоби захисту являють собою організаційно-технічні й організаційно-правові заходи, здійснювані в процесі створення й експлуатації устаткування для забезпечення захисту інформації. Організаційні заходи охоплюють усі структурні елементи устаткування на всіх етапах їхнього життєвого циклу (будівництво помешкань, проектування системи, монтаж і наладка устаткування, іспити й експлуатація).

Безпека інформації забезпечується застосуванням комплексу прийомів, що можна класифікувати в такий спосіб:

- організація охорони помешкань у тому числі з застосуванням систем радіосигналізації; забезпечення безпеки комп'ютерних систем програмними й апаратними засобами;
- періодичне тестування помешкань методами нелінійної радіолокації;
- забезпечення захищеності від прослуховування засобів мобільного радіозв'язку;
- забезпечення акустичної безпеки помешкань і персоналу;
- криптографічні заходи.

Інженерно-технічні засоби реалізуються у вигляді автономних пристроїв і систем і виконують функції загального захисту об'єктів, на яких опрацьовується інформація. До них ставляться, наприклад, пристрої захисту територій і будинків, замки на дверях, де розміщене устаткування, грати на вікнах, електронно-механічне устаткування охоронної сигналізації.

Під **апаратними технічними засобами** розуміють пристрої, що вбудовуються безпосередньо в обчислювальну техніку, або компонуються разом з нею. В наш час існує широкий спектр таких приладів, але найбільшого використання набули такі:

- спеціальні регістри для збереження реквізитів захисту: паролів, кодів ідентифікації, грифів або рівнів секретності;
- пристрої для вимірювання індивідуальних біометричних характеристик людини з метою ідентифікації;
- схеми переривання передачі інформації в лінії зв'язку з метою періодичної перевірки адреси видачі даних;
- пристрої для шифрування інформації (криптографічні методи).

Програмні засоби складають сукупність програмного забезпечення, для ідентифікації користувачів, контролю доступу, шифрування інформації, знищення тимчасових файлів, тестового

контролю системи захисту та інше. Використання програмних засобів захисту інформації має цілий ряд переваг – універсальність, гнучкість, надійність, простота у використанні то можливість модифікації.

Проте, також варто пам’ятати і про людський фактор, на який зловмисники найчастіше орієнтуються. Необережність, цікавість або неуважність користувача можуть звести нанівець всю систему захисту.

Види загроз (атак) інформаційної безпеки та протидія їм.

Метою атаки на будь-які об’єкти є отримання користі або прибутку від отриманих даних. В результаті усі атаки можна поділити на групи з певною цілю.

1. Заміна, модифікація конфіденційної інформації, або крадіжка персональних даних.
2. Отримання доступу до інформації.
3. Перехват інформації.
4. Блокування роботи технічних засобів, або атака на відмову в обслуговуванні.

В таблиці 2 наведено цілі атак та способи їх реалізації

Таблиця 2

Способи реалізації атак щодо цілей

Заміна, модифікація конфіденційної інформації, або крадіжка персональних даних	Отримання доступу до інформації.	Перехват інформації.	Блокування роботи технічних засобів, або атака на відмову в обслуговуванні.
Man-in-the-Middle	Віруси, троянські коні, поштові хробаки,	Аналізатори протоколів (sniffers)	Атака листами (спам)
SQL-ін'єкція, Cross Site Scripting	Мережева розвідка	Man-in-the-Middle	DOS/DDOS атаки
Phishing-атаки	IP-спуфінг		Атаки “Ping of Death”

Перш за все, для протидії атаки варто задіяти методи фізичного перешкоджання шляху зловмиснику до інформації, створити перешкоду. Для цього використовують технічні засоби знімання інформації і дії на неї.

Наступним кроком є методи по управлінню доступом, що включає наступні функції захисту: ідентифікація користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об’єкту персонального ідентифікатора); аутентифікація об'єкту або суб'єкта після пред'явленому їм ідентифікатору; захист Web-додатків за допомогою S-HTTP і SSL-протоколів; захист електронної пошти за допомогою стандартів: PEM, S/MINE, PGP; захист мереж міжмережевими екранами.

На кожен вид потенційної атаки застосовують свої способи протидії.

Проблема з SQL-ін'єкціями вирішується приведенням цілих і дробових величин, перед їх використанням в запиті до потрібного типу.

Мінімізацію появи Phishing-атаки частково вирішують використанням тільки перевірених ресурсів і шляхів доступу до них, а також використанням антивірусних засобів.

Проблему з троянськими програмами, вірусами, поштовими хробаками певною мірою вирішує використання антивірусних засобів і регулярне оновлення їх сигнатур.

Проблему з мережевою розвідкою вирішують відключенням відлуння ICMP і відлуння відповіді на периферійних маршрутизаторах, та використанням систем виявлення проникнень.

Проблему з IP-спуфінгом в повній мірі вирішити не можливо. Застосування криптографічної аутентифікації, фільтрації RFC 2827, та контролю доступу частково послабить дану проблему.

Проблему з сніфферами частково можна вирішити шифруванням даних, що передаються, використанням антисніфферів, міжмережевих екранів.

Вирішення проблеми з атакою Man-in-the-Middle є шифрування потоку інформації.

Загроза атак типу DOS/DDOS може знижуватися трьома способами:

- Функції анти-спуфинга. Правильна конфігурація функцій анти-спуфинга на маршрутизаторах і міжмережевих екранах допоможе знизити ризик DOS. Ці функції, як мінімум, повинні включати фільтрацію RFC 2827.

- Функції анти-DOS. Правильна конфігурація функцій анти-DOS на маршрутизаторах і міжмережевих екранах може обмежити ефективність атак. Ці функції часто обмежують число напіввідкритих каналів в будь-який момент часу.

- Обмеження обсягу трафіку (швидкість трафіку обмеження). Організація може попросити провайдера обмежити обсяг трафіку. Цей тип фільтрації дозволяє обмежити обсяг некритичного трафіку, що проходить по мережі [9].

Рішенням проблеми з атакою "Ping of Death" є введення додаткової перевірки розміру зібраного пакета при отриманні, яка підсумовує зміщення фрагментації всіх пов'язаних пакетів. Якщо загальна сума перевищить 65 535, пакет вважається неправильним і відкидається. Подібна перевірка може проводитися і в міжмережевих екранах.

Висновки. Таким чином, на основі проведеного аналізу методів та способів несанкціонованого доступу в сучасних інформаційних системах та мережах проведено їх ранжування за цілями атаки. Розглянуто організаційну структуру системи захисту інформації та етапи її реалізації. На основі проведених досліджень виділено основні види атак та недоліки при проектуванні системи захисту інформації, а саме від несанкціонованих дій користувачів і програм; втрати інформації і порушення працездатності комп'ютерної системи та адміністративного управління мережею.

Список використаних джерел:

1. Анин Б. Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. — 384 с.

2. Галицкий А.В. и др. Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2005. - 616 с.

3. Лукацкий А. Обнаружение атак. — СПб.: БХВ-Петербург, 2001. — 624 с.

4. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. НПО "Мир и семья- 95", 1997.

5. Касперски К. Техника сетевих атак. М.: СОЛОН-Р, 2001.

6. Kaspersky Security Bulletin 2015. Основная статистика за 2015 год. [Електронний ресурс]. – Режим доступу: https://securelist.ru/analysis/ksb/27543/kaspersky-security-bulletin-2015-osnovnaya-statistika-za-2015-god– Заголовок з екрану.

7. Global Information Technology Report 2013. Growth and Jobs in a Hyperconnected World / World Economic Forum. [Електронний ресурс]. – Режим доступу: http://reports.weforum.org/global-information-technology-report-2013/#=. – Заголовок з екрану.

8. Global Competitiveness Report 2013. Growth and Jobs in a Hyperconnected World / World Economic Forum. – Geneva Switzerland-2012. [Електронний ресурс]. – Режим доступу: http://reports.weforum.org/global-competitiveness-report-2012-2013/#=– Заголовок з екрану.

9. Боршевнікі А. Е. Мережеві атаки. Види. Способи боротьби [Текст] // Сучасні тенденції технічних наук: матеріали Міжнар. науч. конф. (Г. Уфа, жовтень 2011 року). - Уфа: Літо, 2011. - С. 8-13.

10. P. Resnick, RFC-2821 "Internet Message Format (Proposed Standart)", April 2001.

Стаття надійшла до редакції 29.04.2017