УДК 004.056

Дмитро МУЛ,
кандидат технічних наук, доцент,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

Євгеній ПРОКОПЕНКО,
кандидат технічних наук, доцент,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

Руслан ХОПТИНСЬКИЙ,
кандидат технічних наук,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

АНАЛІЗ ТА ОБҐРУНТУВАННЯ ВИМОГ ДО СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Інформація як сукупність знань про фактичні що дають кількісну характеристику явищ та процесів і залежності між ними стала стратегічним ресурсом; вона – основа для прийняття управлінського рішення. Тому захист інформації як складна, наукомістка і багатогранна проблема в умовах упровадження сучасних інформаційних технологій, створення та супроводження розподілених інформаційних систем набуває особливої гостроти.

Ключові слова: *телекомунікаційна система, політика безпеки, вірусна програма, DDoS-атака, інформаційна безпека.*

Постановка проблеми у загальному вигляді. Питання безпеки – невід'ємна частина концепції впровадження нових інформаційних технологій у Стратегії розвитку Державної прикордонної служби України. Широкомасштабне впровадження автоматизованих робочих міць різних типів і корпоративної телекомунікаційної мережі Інтранет у межах Інтегрованої інформаційно-телекомунікаційної системи "Гарт", збільшення обсягів інформації, яка обробляється, і розширення кола користувачів приводять до якісно нових можливостей несанкційованого доступу до ресурсів і даних інформаційної системи, до їх високої вразливості [2]. Основними вимогами до забезпечення захисту інформаційних ресурсів є : цілісність, достовірність і доступність інформації. Ефективність механізмів захисту інформації значною мірою залежить від реалізації ряду принципів. По-перше, розробку системи політики безпеки доцільно проектувати одночасно з розробкою інформаційної системи, що дозволяє забезпечити їхню безконфліктність, своєчасну інтеграцію в інформаційне середовище і скорочення витрат. По-друге, питання захисту варто розглядати комплексно в рамках єдиної корпоративної системи захисту інформації.

Аналіз останніх досліджень і публікацій. Було вивчено та проаналізовано ряд методик, які використовувались раніше для оцінки ефективності системи захисту корпоративних телекомунікаційних мереж [4, 5, 6]. Ці методики виявились дуже громіздкими та не давали можливість ефективно оцінити політику безпеки мереж за всіма показниками, які її характеризують.

Це дає змогу використати такі показники, які з достатнім ступенем точності дозволили би охарактеризувати ефективність політики безпеки корпоративної телекомунікаційної мережі Держприкордонслужби Інтранет.

Метою статті є аналіз політики безпеки корпоративних телекомунікаційних мереж та обґрунтування вимог до системи захисту.

Виклад основного матеріалу дослідження. Функціонування Державної прикордонної служби, як і України загалом, в умовах військо-

вої агресії з боку Російської Федерації на східному кордоні України підкреслює важливість забезпечення прихованості та достовірного інформаційного обміну в системі управління.

Саме системний підхід може забезпечити адекватний багаторівневий захист інформації, що розглядається як комплекс організаційно-правових і технічних заходів. Крім того, при реалізації механізмів захисту повинні використовуватися передові, науково обґрунтовані технології захисту, що забезпечують необхідний рівень безпеки, прийнятність для посадових осіб і можливість нарощування і модифікації політики безпеки для інформації.

Масштабна хакерська атака, яка відбувалась у декілька етапів і призвела до блокування діяльності таких підприємств, як аеропорт "Бориспіль", ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та низки інших великих підприємств, розпочалась 14 квітня 2017 року з компрометації системи оновлення програми M.E.Doc [3]. Останній етап з використанням різновиду вірусу Petya відбувся 27 червня 2017 року та спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Масштабна деструктивна атака різновидом вірусу Petya (також відомого як NotPetya, Eternal Petya, Petna, ExPetr тощо) стала можливою через компрометацію системи оновлення програми M.E.Doc та встановлення прихованого бекдору. Таким чином, масштабною деструктивною атакою зловмисники закрили собі наявний в них завдяки бекдору доступ до комп'ютерів та комп'ютерних мереж у близько 80 % українських підприємств (в тому числі представництв закордонних компаній). Є підстави вважати, що зловмисники пішли на такий крок, оскільки або здобули надійніший доступ до інформаційних систем важливих для них жертв, або ж вважали, що зможуть доволі просто відновити його.

Бекдор (від англ. back door, чорний хід), люк в комп'ютерній системі (криптосистемі або алгоритмі) – це метод обходу стандартних процедур аутентифікації, несанкційований віддалений доступ до автоматизованого робочого місця, отримання доступу до відкритого тексту тощо, залишаючись при цьому непоміченим.

Ще одним прикладом порушень інформаційної безпеки є атаки з розподіленою відмовою в обслуговуванні – це реальна і зростаюча

загроза, з якою стикаються компанії у всьому світі. Ці атаки реалізуються великою кількістю програмних агентів, розміщених на хостах, які зловмисник скомпрометував раніше. Реалізація цих атак може призвести не тільки до виходу з ладу окремих хостів і служб, а й зупинити роботу кореневих DNS-серверів і викликати часткове або повне припинення роботи корпоративної телекомунікаційної мережі. У зв›язку з критичністю і нетривіальністю даного класу атак побудова ефективних засобів захисту від них являє собою складну науково-технічну проблему. На рівні маршрутизаторів захист від DDoS-атак вже досить успішно реалізовували компанії Cisco Systems і Arbor Networks. Але в цілому проблема DDoS-атак на сьогоднішні, як і раніше, дуже гостро стоїть для більшості компаній.

DoS-атака (від англ. Denial of Service, відмова в обслуговуванні) – атака на обчислювальну систему з метою вивести її з ладу, тобто створення таких умов, за яких легітимні (правомірні) користувачі системи не можуть отримати доступ до надаваних системою ресурсів, або цей доступ ускладнений [1].

Атаку на відмову в обслуговуванні можна провести трьома способами:

використовуючи вразливості в програмному забезпеченні;

посилаючи мережний трафік на атаковану систему, що значно перевищує її пропускну здатність;

завантажуючи до максимально можливої продуктивності критично-важливі системні ресурси атакованої системи: процесорний час і пам’ять.

Звичайно, один комп’ютер не може переповнити канал сервера, тому для цього використовується розподілена атака “відмова в обслуговуванні”.

DDoS-атака має ієрархічну структуру – трирівневу модель, що складається з таких елементів:

консолі управління, тобто головного комп’ютера, що подає сигнал про те, що розпочалась атака;

“комп’ютерів-демонів”, які, отримавши сигнал від консолі управління, передають його “ураженим машинам”;

атакуючих агентів – керованих заражених комп'ютерів, що посилають запити на кінцеву мішень.

Загальна схема ієрархічної структури DDoS-атаки зображена на рисунку. Простежити таку структуру в зворотному напрямку і виявити адресу сайту, який організував атаку, практично неможливо. Максимум, що можна зробити, – це визначити адреси агентів, які атакують сервер. Спеціальні заходи в кращому разі приведуть до "комп'ютера-демона". Але в даній ситуації комп'ютери-агенти і "комп'ютери-демони" самі є постраждалими (скомпрометованими).

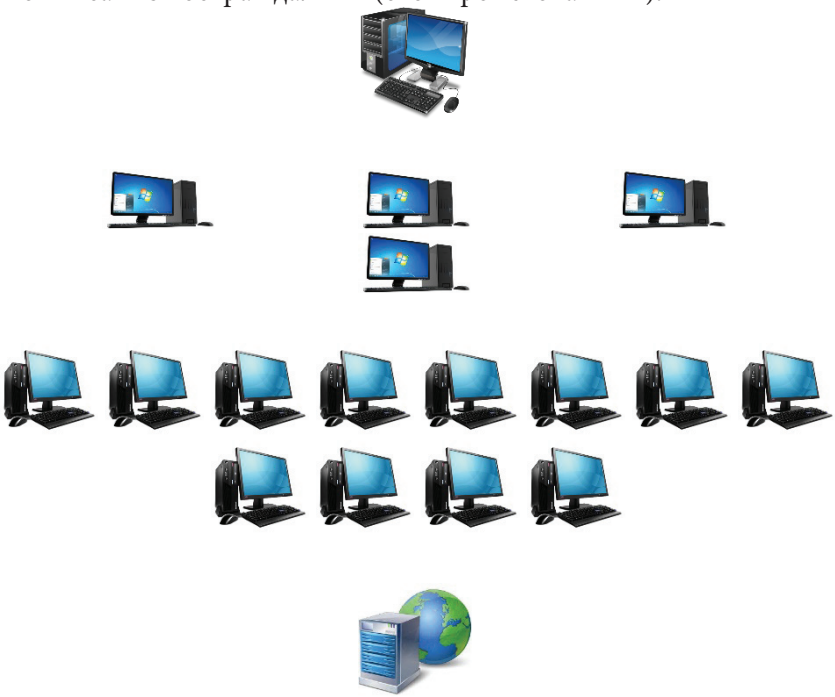

Схема ієрархічної моделі DDoS-атаки

Вірусна мережа створюється шляхом зараження автоматизованого робочого місця троянською програмою. Ця програма потрапляє на комп'ютер користувача, найчастіше у разі необережного поводження з електронною поштою, наприклад, відкриття вкладень у листах, або

при відвідуванні зараженого сайту, коли зловмисник може, використовуючи вразливості браузера або операційної системи, встановити на комп'ютер користувача шкідливе програмне забезпечення. Така програма може протягом тривалого часу нічим деструктивним себе не виявляти. Часто власник комп'ютера навіть не підозрює, що його машина заражена і повністю підконтрольна комусь невидимому.

За відповідною командою до атаки мережа заражених машин починає працювати. Запити йдуть з багатьох точок мережі, йдуть з високою частотою, і сайт, який вони атакують, починає не справлятися з великим потоком звичайних запитів, перестає відповідати на легітимні запити і блокується [5, 6].

DDoS-атаки можна класифікувати таким чином:

переповнення смуги пропускання каналу зв'язку (bandwidth consumption). Ці атаки засновані на тому, що атакуючий заповнює смугу пропускання каналу. Відповідно, забитий канал не може пропустити до сервера ще які-небудь інші запити. Інформація з сервера стає тимчасово не доступною для користувачів.

нестача ресурсів (resource starvation). Атаки спрямовані на захоплення критичних системних ресурсів: процесорний час, місце на диску, пам'ять тощо. Результат – усі інші процеси не можуть виконуватись, а користувачі не можуть отримати доступ до сервісів;

помилки програмування (programming flaw). Ці атаки спрямовані на слабкі місця, програмні помилки, закладені випадково при розробці, і недокументовані функції операційних систем, програмного забезпечення, процесорів і програмованих мікросхем. Знаючи слабкі місця в чомусь з вищепереліченого, можна створити і відправити за призначенням певний пакет, який викличе помилку, переповнення буфера або стека;

маршрутизація і DNS. Якщо мати доступ до маршрутизатора, то можна змінити таблиці маршрутизації таким чином, щоб бажаючі потрапити на сервер з визначеною IP адресою потрапляли зовсім на іншу IP адресу або на IP, якого взагалі не існує. Те ж саме DNS, але вже щодо сайтів. Якщо отримати доступ до кешу DNS, можна прив'язати шукане доменне ім'я зовсім до іншого IP адресу, і тоді користувачі

будуть потрапляти на цей самий зовсім інший сервер, а не туди, куди вони хотіли. Якщо ж вкласти взагалі неіснуючий IP, то це буде більше схоже на DoS;

flood. Цей тип можна віднести до попередніх DoS, але виділимо його окремо. З деякої кількості машин посилають жертві максимально можливу кількість запитів (наприклад, запити на з'єднання). Від цього жертва не встигає відповідати на кожен запит і в результаті не відповідає на запити користувачів, тобто перестає нормально функціювати.

Боротьба з розподіленими DoS-атаками – справа досить непроста. По-перше, дуже важко встановити організатора атаки, а користувачі, чиї комп'ютери генерують паразитичний трафік, як правило, навіть не підозрюють, що їхні машини стали інструментом в руках зловмисників. По-друге, практично неможливо відрізнити шкідливий трафік від легітимного, оскільки по суті це ті ж самі запити, що і від звичайних користувачів, але в надзвичайно великій кількості.

Аналіз аномалій у мережному трафіку – єдиний ефективний метод виявлення DDoS-атаки. З точки зору захисту, DDoS-атаки є однією з найбільш складних мережних загроз, тому прийняття ефективних заходів протидії є виключно складним завданням.

Вчасно виявити DDoS-атаку – у цьому і полягає головна проблема, якщо ми не хочемо боротися з нею за фактом падіння ресурсів мережі.

Найбільш ефективний спосіб виявити DDoS-атаку заснований на накопиченні статистичних даних про проходження трафіку в мережі. Склавши картину нормального стану мережі, завжди можна відстежити виникнення якої-небудь аномалії в мережному трафіку.

Як джерело даних для статистики можна використовувати сам трафік або деяку статистичну інформацію про нього. Для цього використовуються додаткові маркери мережі, які можуть надати інформацію про неї.

У загальному випадку система за відсутності DDoS-атак на захищений ресурс проходить етап тестування або навчання. Система визначає і запам'ятовує, який трафік для захищеного ресурсу є нормальним. Ситуація, за якої поточний трафік на захищений ресурс

різко відрізняється від нормального, вважається DDoS-атакою. Варто підкреслити, що система розпізнає тільки відхилення від трафіку, а чим він викликаний – сплеском легітимних звернень до ресурсів або DDoS-атакою, – може визначити лише власник ресурсу: очікував він такий обсяг звернень чи ні [1].

Після виявлення факту аномалії відбувається її класифікація і визначається, наскільки вона серйозна. Якщо DDoS-атака не загрожує виникненням проблем у мережі, то краще спостерігати і нічого не робити, оскільки виникає ймовірність не пустити на ресурс законного користувача.

Технічна реалізація даного рішення передбачає наявність у мережі двох додаткових пристроїв, один з яких здійснює моніторинг вхідного трафіку і виявляє проведення DDoS-атаки, а другий фільтрує (очищає) вхідний ззовні трафік.

Висновки дослідження перспективи подальших розвідок у даному напрямку. У статті автором проведено дослідження стану інформаційної безпеки сучасних телекомунікаційних мереж, оцінено загрози та можливий вплив на функціонування корпоративної мережі Держприкордонслужби Інтранет. Однією зі зростаючих загроз порушень інформаційної безпеки є атака з розподіленою відмовою в обслуговуванні. На сьогодні існує багато способів захисту, але всі вони не універсальні і не вирішуються відразу для всіх завдань при відбитті скільки-небудь потужного DDoS.

Проблема забезпечення інформації безпеки з погляду державних інтересів останнім часом набула особливої актуальності і розглядається як одне з пріоритетних державних завдань – як важливий елемент національної безпеки.

Список використаної літератури:

1. DoS-атака. – Режим доступу : https://ru.wikipedia.org/wiki/DoS-атака

2. Про схвалення Стратегії розвитку Державної прикордонної служби : постанова КМУ від 23 листопада 2015 р. № 1189-р.

3. Про захист інформації в інформаційно-телекомунікаційних системах Закон України.

4. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

5. Орленко В. С. Методи оцінки та підвищення захищеності інформаційних ресурсів систем спеціального призначення : автореферат на здобуття наукового ступення кандидата технічних наук, Державний університет інформаційно-комунікаційних технологій. – К., 2009.

6. Талалаєв В. О., Стороженко О. В. Світові тенденції розвитку телекомунікаційних мереж військового призначення // Інформаційний збірник по зв'язку. – 2005. – № 4. – С. 79–88.

Рецензент – доктор технічних наук, професор Андрощук О. С.

Мул Д., Прокопенко Є., Хоптинский Р. **Анализ и обоснование требований к системе защиты корпоративной телекоммуникационной сети**

В статье исследуются вопросы обоснования требований к системе защиты корпоративной телекоммуникационной сети Интранет. Информация как совокупность знаний о характеристике явлений, процессов и зависимости между ними стала стратегическим ресурсом, она является основой для принятия управленческого решения. Поэтому защита информации как сложная, наукоемкая и многогранная проблема в условиях внедрения современных информационных технологий, создание и сопровождение распределенных информационных систем приобретает особую остроту.

Ключевые слова: *телекоммуникационная система, политика безопасности, вирусная программа, DDoS-атака, информационная безопасность.*

Mul D., Prokopenko Y., Khoptynskyi R. **Analysis and justification of the requirements for the protection system of the corporate telecommunication network**

The article explores the issues of substantiating the requirements for the protection system of the corporate intranet telecommunications network. Information as a body of knowledge about the characteristics of phenomena, processes and relationships between them, has become a strategic resource - it is the basis for making managerial decisions. Therefore, the protection

of information as a complex, knowledge-based and multifaceted problem in the context of the introduction of modern information technologies, the creation and maintenance of distributed information systems becomes particularly acute.

The functioning of the State Border Service, as the Ukraine, emphasizes the importance of secrecy and reliable information exchange in the management system.

It is the systematic approach that can provide adequate multi-level information protection, is considered as a complex of organizational, legal and technical measures. In addition, when implementing protection mechanisms, advanced, scientifically based protection technologies should be used that ensure the necessary level of security, and the possibility of building and modifying the security policy for information.

The problem of ensuring information security from the point of view of the state interests has recently become particularly relevant and considered as one of the priority state tasks - an important element of national security.

Keywords: *telecommunication system, security policy, virus program, DDoS-attack, information security.*