УДК 004.7.056

Г. В. Бабенко

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ВОЗНИКАЮЩИХ ПРИ СЕТЕВОМ ВЗАИМОДЕЙСТВИИ

Введение

Количество случаев нарушения информационной безопасности в компьютерных сетях ежегодно увеличивается. Системы антивирусного контроля, программные и аппаратные межсетевые экраны все больше оказываются неспособными к предотвращению негативных последствий от реализации различных угроз безопасности информации при межсетевом взаимодействии.

Острой проблемой становится неспособность или невозможность средств защиты реагировать на так называемее угрозы «нулевого дня». Эти угрозы, как правило, не обнаруживаются, т. к. традиционные средства защиты не обладают о них необходимой информацией.

Для построения эффективных средств защиты необходимо разработать алгоритм классификации возникающих угроз, представить схемы их реализации, выявить цели, на которые они направлены, т. е. провести анализ угроз безопасности информации и их компонент.

Классификация угроз

Для классификации угроз в первую очередь необходимо разработать *общую схему сетевого взаимодействия*, расположения сетей, компонентов сетевой инфраструктуры относительно потенциальных нарушителей (рис. 1).

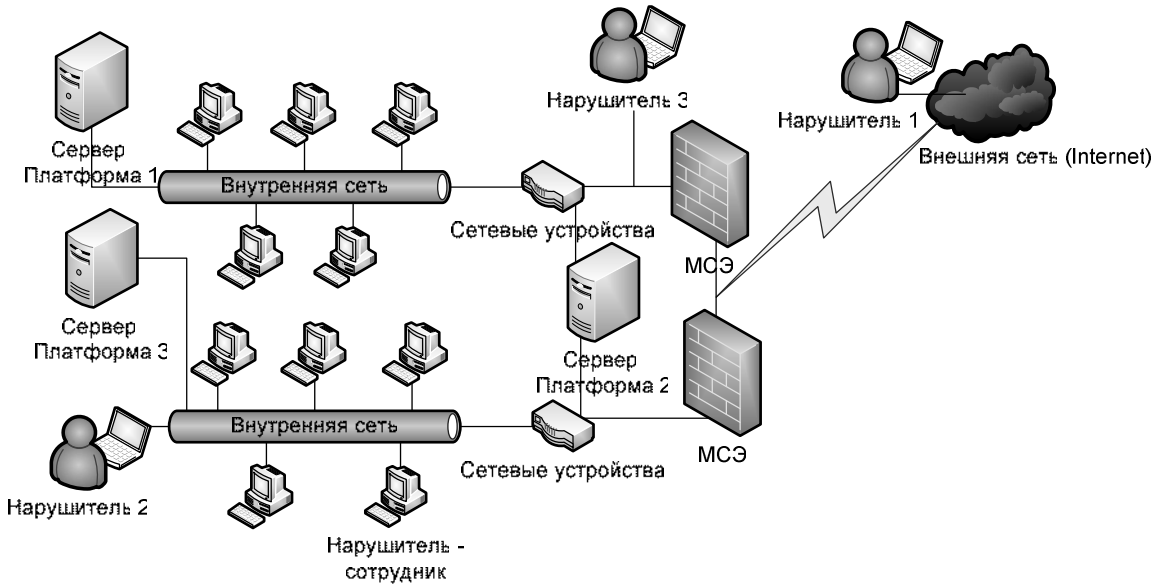

Рис. 1. Схема расположения сетей и потенциальных нарушителей: МСЭ – межсетевой экран

В соответствии со схемой необходимо определить уязвимые звенья системы.

Систему условно можно разделить на три класса уязвимых звеньев (УЗ):

– программные УЗ;
– аппаратные УЗ;
– антропогенные УЗ.

Далее каждому классу УЗ в процессе анализа необходимо сопоставить потенциальные угрозы безопасности информации.

Анализ угроз

Для анализа угроз безопасности информации при сетевом взаимодействии применим методику структуризации целей и функций [1].

Представим совокупность УЗ и угроз безопасности как систему, состоящую из шести уровней (рис. 2), где верхние составляющие – цели, а нижние – функции, исключая уровень жизненного цикла:

- формирование глобальной цели;
- виды конечного продукта;
- пространство инициирования целей;
- жизненный цикл;
- основные характеристики системы;
- управленческий цикл.

Рис. 2. Схематичное отображение системы

Основной (глобальной) целью будут являться нарушения основных свойств информации:

1. Нарушение целостности и достоверности передаваемой информации.
2. Нарушение конфиденциальности передаваемой информации.
3. Нарушение доступности информации, системы в целом или отдельных ее частей.

Видами конечного продукта будут являться классы УЗ, определенные выше:

1. Программные УЗ.
2. Аппаратные УЗ.
3. Антропогенные УЗ.

Пространством инициирования целей будут являться конкретные компоненты системы, влияние на которые может привести к тому или иному конечному результату. Для этого определим типы УЗ:

1. Операционные системы (ОС) и компоненты/надстройки.
2. Программные системы/средства защиты информации (ПСЗИ).
3. Прикладное программное обеспечение (ПО).
4. Настройки и конфигурации аппаратных компонент сетевой инфраструктуры.
5. Линии передачи информации.
6. Компоненты сетевой инфраструктуры (коммутаторы, маршрутизаторы, конверторы и т. д.).
7. Аппаратные системы/средства защиты информации (АСЗИ).
8. Локальные рабочие станции (ЭВМ).
9. Различные действия сотрудников и пользователей.

Жизненный цикл – это совокупность этапов получения конечных продуктов в зависимости от их видов:

1. Появление необходимости (потребности) в использовании или введении конкретного УЗ.
2. Производство (создание) при отсутствии такового либо аналогов.

3. Транспортировка.
4. Внедрение в инфраструктуру.
5. Настройка.
6. Использование по функциональному назначению (эксплуатация).

Состав системы – функции, вытекающие из потребностей основных характеристик системы. Элементы системы могут обладать как парой характеристик, так и отдельно взятой характеристикой:

1. Непреднамеренные/преднамеренные.
2. Случайные/целенаправленные.
3. Внешние (удаленные)/внутренние.
4. Активные/пассивные.
5. Условные/безусловные.
6. Организационные/программно-аппаратные, технические.
7. С обратной связью/без обратной связи.
8. С физическим доступом/без физического доступа.
9. Автоматические/автоматизированные.
10. С наличием «наследования»/без наличия «наследования».
11. Контролируемые/неуправляемые.
12. Распределенные/централизованные.
13. Информационно-разведочные/деструктивные.

Управленческий цикл – непосредственно функции и действия, осуществляемые для достижения глобальной цели:

1. Навязывание необходимости приобретения, разработки, введения новых компонентов.
2. Случайные ошибки при проектировании, производстве и эксплуатации.
3. Намеренное внедрение нерегламентированных возможностей.
4. Случайный сбой, отказ аппаратных или программных средств.
5. Доступ к информации с использованием программно-аппаратных закладок.
6. Доступ к информации при передаче по линиям связи (программный перехват телекоммуникационного трафика, физическое внедрение в инфраструктуру и т. д.).
7. Уничтожение или хищение носителя информации, средств обработки и коммуникации.
8. Изменение параметров BIOS на локальных рабочих станциях.
9. Загрузка альтернативных ОС и ПО с нештатных носителей.
10. Получение критически важных данных (имен пользователей и паролей), при помощи brute-force воздействий (полный перебор) либо специализированного ПО.
11. Изменение различных параметров ОС (создание новых учетных записей, редактирование реестра, параметров загрузки, групповых политик и т. д.).
12. Нарушение корректной работы ОС.
13. Установка опасного прикладного ПО.
14. Сканирование сетевой инфраструктуры – «апробирование порта» (определение сетевого адреса (IP-адреса), идентификация открытых портов, запущенных служб, определение типа ОС и сетевых компонент) [2].
15. Сбор системной информации (идентификация системного ПО, совместно используемых ресурсов, учетных записей и т. п.).
16. Внедрение ложного доверенного объекта (подмена таблицы преобразования адресов – ARP spoofing, подмена сетевого адреса – IP-spoofing, подмена сервера доменной системы имен – DNS spoofing) [3].
17. Угрозы удаленного перехвата сетевого трафика.
18. Выявление конфигурационной информации сетевых устройств.
19. Переполнение буфера с запуском исполняемого кода.
20. Инсталляция (запись) ПО с последующим запуском других инсталяционных процессов (инсталляция ПО, расширяющего привилегии пользователя, разрушающего аппаратное обеспечение компьютера, инсталляция и запуск вируса, инсталляция программ удаленного управления).
21. Перенаправление сетевого трафика (изменение таблиц маршрутизации на сетевых устройствах, передача ложных пакетов протокола маршрутизации (RIP)) [4].
22. Атаки на пользователей Интернет-сервисов [5].

23. Отказы в обслуживании (DoS) (отказ в обслуживании на хосте пользователя, угрозы отказа в обслуживании на сервере доменных имен (DNS-сервер), отказ в обслуживании на маршрутизаторе, вспомогательных серверах).

24. Преодоление АСЗИ или ПСЗИ.

В данный перечень включены все угрозы, за исключением угроз несанкционированного доступа к информации с применением технических каналов утечки информации, не использующих методы передачи информации в TCP/IP сетях, а также угроз, являющихся вторичными по отношению к вышеуказанным.

Заключение

В нашей попытке описания основных угроз безопасности информации, циркулирующей в компьютерных сетях, совокупность угроз представлена как многоуровневая система. Проведена их классификация, описаны схемы их выполнения и возможные последствия от их успешной реализации. Результаты исследования позволяют сделать некоторые выводы: на этапе эксплуатации вероятность возникновения угрозы имеет самое высокое значение; ошибки, допущенные на этапе настройки, влекут за собой существенный рост вероятности возникновения угрозы во время эксплуатации; количество УЗ напрямую зависит от размеров и инфраструктуры сети; наличие СЗИ снижает вероятность успешной реализации угроз, но не гарантирует их полное отсутствие; человеческий фактор играет большую роль в процессе обеспечения безопасности. Однако методы и способы нарушения безопасности совершенствуются: изменяются исходные условия, время, затраченное на их выполнение. В результате совершенствуются и средства защиты, однако в большинстве случаев злоумышленникам удается их обходить, применяя методы, которые до определенного времени неизвестны средствам защиты.

СПИСОК ЛИТЕРАТУРЫ

1. *Болотова Л. С., Волкова В. Н., Денисов А. А.* Теория систем и системный анализ в управлении организациями: Справочник: учеб. пособие / под ред. В. Н. Волковой и А. А. Емельянова. – М.: Финансы и статистика, 2006. – 848 с.
2. *Шаньгин В. Ф.* Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008. – 544 с.
3. *Андрончик А. Н., Богданов В. В., Домуховский Н. А.* Защита информации в компьютерных сетях. Практический курс: учеб. пособие / под ред. Н. И. Синадского. – Екатеринбург: УГТУ – УПИ, 2008. – 248 с.
4. *Заклянов П.* Обнаружение телекоммуникационных атак: теория и практика // Системный администратор. – 2005. – № 10. – С. 48–67.
5. *Биячуев Т. А.* Безопасность корпоративных сетей / под ред. Л. Г. Осовецкого. – СПб.: СПбГУ ИТМО, 2004. – 161 с.

Статья поступила в редакцию 12.03.2010

ANALYSIS OF MODERN THREATS TO INFORMATION SECURITY OCCURRING WHILE THE NETWORK INTERACTION

G. V. Babenko

The classification of information security threats from networking was based on the general scheme of networking, networks location, network infrastructure components relative to potential offenders. Furthermore, three classes of vulnerable parts of the system (software, hardware, man-made) were identified for convenience. The structuring method of objectives and functions was used for the analysis. According to it, the set of vulnerable sections and security threats is represented as a system of six levels, where the upper components – goals, and the bottom ones- functions, except for the level of the life cycle. The result is a system, where each vulnerable part can be compared with the list of threats to information security.

Key words: vulnerability, network interaction, threats to information security, structuring of objectives and functions, operation system, network infrastructure, means of information security, privacy, availability, integrity.