УДК 004.942
DOI: 10.33764/2618-981X-2021-6-52-57

ИССЛЕДОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ НА НАЛИЧИЕ УЯЗВИМОСТИ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНОЙ СРЕДЫ

Роман Сергеевич Горохов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (999)463-43-96, e-mail: roma_gorohov2013@mail.ru

Игорь Николаевич Карманов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой физики, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

В работе рассмотрены варианты обследования локально-вычислительной сети организации на внешние источники доступа. Описаны подходы поиска точек взаимодействия потенциального злоумышленника с системой. Также предложен вариант решения проблемы невозможности использования действующей информационной системы путем использования виртуальной среды. Таким образом, появляется возможность проводить тестирование информационной системы на наличие угроз безопасности на максимально приближенном к реальности макете.

Ключевые слова: безопасность, защита, информация, информационная система

TESTING INFORMATION SYSTEM OF AN ENTERPRISE FOR VULNERABILITY USING VIRTUAL ENVIRONMENT

Roman S. Gorohov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (999)463-43-96, e-mail: roma_gorohov2013@mail.ru

Igor N. Karmanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph.D, Associate Professor, Head of the Department of Physics, phone: (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

The paper focused on options for examining the organization's local area network for external sources of access. The approaches to finding the points of interaction of a potential attacker with the system are described. A variant of solving the problem of the impossibility of using the existing information system by using a virtual environment is also proposed. Thus, it becomes possible to test the information system for the presence of security threats, on a model that is as close to reality as possible.

Keywords: security, protection, information, information system

Введение

Исследования информационных систем направлены на изучение процессов, связанных с разработкой, развертыванием и эксплуатацией информационной системы (ИС) на предприятии. Таким образом, чтобы лучше понять природу про-

исходящего внутри ИС, может быть полезно изучить процессы работы в естественной обстановке, понаблюдать за работой и поведением человека внутри системы. В частных случаях задача состоит в том, чтобы охватить весь процесс работы организации и ИС, для получения полной картины. Но чаще всего перед исследователем стоит конкретная задача, связанная с наблюдением и сравнением повторяющегося примера одного и того же процесса.

Рассматривая работу предприятия, будем акцентировать внимание на работе ее информационной системы. В организации с использованием ИС в полной мере перед работниками открываются безграничные возможности по использованию технологий для обеспечения большой скорости работы. Таким образом, можно утверждать, что сотрудник может обмениваться необходимыми документами внутри организации с большой скоростью, для работы материалы могут быть получены сотрудником моментально из единой базы данных. Подобный вариант взаимодействия сотрудника с ИС делает работу организации более эффективной. Чаще всего в подобных сетях не обходится без подключения к ИС связи общего пользования. Из вышесказанного можно сделать вывод, что использование подобных информационных технологий делает актуальной проблему защиты информации [3, 5].

Работа исследователя заключена в моделировании ИС предприятия. Сегодня технологии виртуализации используются повсеместно и вплетены практически во все технические области. Это позволяет использовать такой подход для проведения работ по анализу ИС на соответствие требованиям информационной безопасности (ИБ).

Перед началом исследования необходимо разобраться в структуре организации, проанализировать все аспекты, которые угрожают безопасности. Для этого нужно знать, какая политика разработана для защиты ИБ на предприятии. Далее получить имеющийся анализ рисков, составленный организацией, для того чтобы иметь представление о вероятности реализации угроз, учесть, какие программные комплексы используются организацией для обеспечения работоспособности системы и информационной безопасности.

Изучив вышеуказанные моменты, связанные с обеспечением ИБ, необходимо провести анализ информации, обрабатываемой в ИС, определить, какие данные необходимо защищать. К данным, помимо информации, обрабатываемой в системе, также могут относиться данные, связанные с внутренней деятельностью организации (регистрационные данные пользователя в системе, личные карточки сотрудников и т.д.) [10].

Методика анализа

На данный момент не предложен общепринятый метод поиска уязвимости. Однако можно выделить список контрмер, направленный на конкретные узлы и уязвимости, связанные со сложными методами, а также действиями, которые традиционно воспринимаются как протоколы безопасности. Примерный список методов можно представить в виде последовательности действий, которые необходимо выполнить исследователю ИС. Такой порядок действий представлен на рис. 1.

Рис. 1. Предложенный порядок анализа безопасности ИС

Чтобы смягчить и уменьшить количество атак, упомянутые контрмеры должны использоваться в зависимости от их эффективности в снижении уязвимостей.

В работе представлен вид тестирования, который может быть использован для сертификации объекта исследования. Он представляет собой метод тестирования безопасности на основе реальных действий нарушителя. В данном случае будут учтены способы взаимодействия нарушителя с уязвимостями и их эксплуатации. В итоге необходимо получить отчет о реальной угрозе эксплуатации нарушителем найденной уязвимости [9].

Чтобы не навредить действующей ИС предприятия, современные информационные технологии дают возможность производить проверку наличия уязвимости системы, не используя ее физическую составляющую [4]. Для этого существующая сеть моделируется в виртуальной среде. В нее входят компоненты, предназначенные для функционирования тестируемой системы. Поскольку в каждой ИС используется программное обеспечение, необходимое для осуществления деятельности определённой организации, это значит, что каждая визуализируемая модель будет так или иначе отличаться от других. Поэтому не стоит забывать, что для полноценной чистоты эксперимента необходимо в полной мере воссоздать весь программный комплекс, используемый в сети предприятия. После подготовки визуализированного проекта можно приступать к тестированию модели на уязвимости.

Исследование системы на поиск уязвимостей делится на несколько этапов (рис. 2).

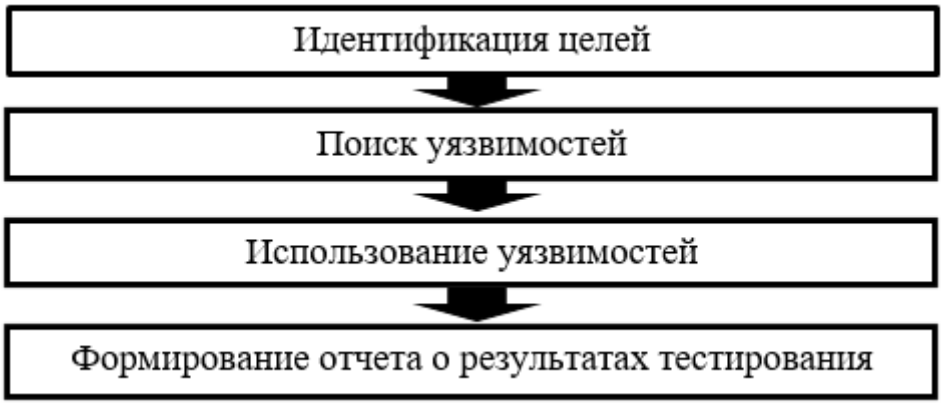

Рис. 2. Методика исследования системы

Чтобы иметь представление о том, что должно происходить на каждом этапе поиска уязвимостей, представим теоритическую попытку проникновения исследователя с возможностью физического доступа к ИС.

Первым делом исследователь ведет поиск, используя сканер сети. Данная операция может позволить увидеть доступные узлы. Это позволяет исследователю узнать, какое устройство скрывается за определенным адресом внутри сети (сервер, база данных (БД), персональный компьютер) [1].

Следующий этап включает в себя выбор объекта исследования. Исследователь выбирает определенный адрес внутри сети, используя на нем сканер сети с БД известных уязвимостей. Таким образом исследователь получает список уязвимостей, которые на следующем этапе использует.

На третьем этапе исследователь использует найденные уязвимости, чтобы продемонстрировать вред, который может принести данная угроза.

Таким образом, используя виртуальную модель ИС, можно получить представление о найденных уязвимостях, провести анализ защищенности сети и устранить их.

Использование виртуальной среды также может помочь на этапе планирования подсистемы защиты, создаваемой ИС. Примерная схема представлена на рис. 3. Планируется, что на рабочих станциях сотрудники обрабатывают конфиденциальную информацию.

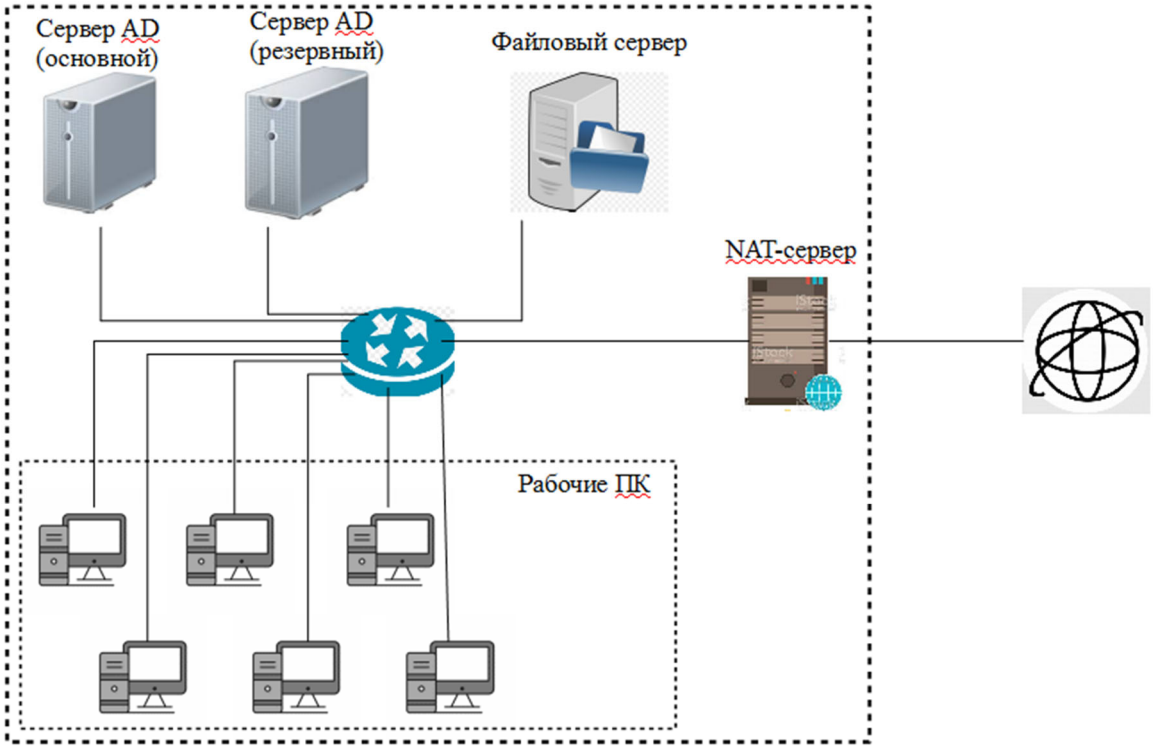

Рис.3. Структурная схема виртуальной ИС

Сервер AD (Active Directory), помимо своей основной роли, является DNS (Domain Name System) и DHCP (Dynamic Host Configuration Protocol) сервером. Резервный сервер AD дублирует основной сервер AD и предназначен для обеспечения отказоустойчивости ИС. NAT-сервер (Network Address Translation) – сервер, который обеспечивает сотрудникам доступ в сеть Интернет. Всем клиентам сети IP-адрес выдается автоматически сервером DHCP. На всех серверах IP-адреса занесены в список исключений на сервере DHCP [2, 6].

Файловый сервер выполняет функцию так называемой «файловой помойки». Предполагается, что на компьютерах сотрудников конфиденциальная информация не хранится, и после работы сотрудника с документом файл переносится на сервер. Предполагается, что такой подход закреплен в организационно-распорядительных документах предприятия [7].

Заключение

Основная цель этой статьи состояла в том, чтобы описать подход к изучению модели поиска уязвимостей в ИС. Таким образом, используя виртуализацию ИС, можно проверить ее на соответствие стандартам безопасности, даже в том

случае, когда нет возможности организовать инструментальный контроль, непосредственно используя физическую сеть предприятия ввиду возможности нарушения работоспособности системы, в которой протекает непрерывный рабочий процесс.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Поляк-Брагинский А. В. Администрирование сети на примерах / А. В. Поляк-Брагинский. – СПб.: БХВ-Петербург, 2005. – 320 с.: ил.

2. Барановская Т.П. Архитектура компьютерных систем и сетей: Учеб. пособие / Т.П. Барановская, В.И. Лойко и др.; под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. – 256 с.: ил.

3. Баринов, Андрей Безопасность сетевой инфраструктуры предприятия / Андрей Баринов. – М.: LAP Lambert Academic Publishing, 2016. – 331 с.

4. Брэгг, Роберта Безопасность сетей. Полное руководство / Роберта Брэгг, Марк Родс-Оусли, Кит Страссберг. – М.: Наука, 2017. – 912 с.

5. Палмер, Майкл Проектирование и внедрение компьютерных сетей / Майкл Палмер, Роберт Брюс Синклер, Майкл Палмер. – СПб.: БХВ-Петербург, 2018. – 740 с.

6. Поляк-Брагинский, А. В. Локальная сеть. Самое необходимое / А.В. Поляк-Брагинский. – СПб.: БХВ-Петербург, 2016. – 576 с.

7. Рассел, Джесси Сервер (программное обеспечение) / Джесси Рассел. – М.: Книга по требованию, 2012. – 114 с.

8. Садердинов, А.А. Информационная безопасность предприятия: учеб. пособие / А.А. Садердинов, В.А. Трайнев, А.А. Федулов. – М.: Дашков и К°, 2005. – 336 с.

9. Семененко, В.А. Информационная безопасность: учеб. пособие / В.А. Семененко.– 4-е изд. – М.: МГИУ, 2010. – 277 с.

10. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – М.: «ФОРУМ»: ИНФРА-М, 2011. – 416 с.