ВВЕДЕНИЕ

Принципы и методы защиты информации в компьютерных сетях подробно излагаются во многих источниках. Вместе с тем ощущается недостаток пособий, в которых защита в компьютерных сетях была бы описана в виде, минимально необходимом и в то же время достаточном для практического освоения основных принципов защиты на примере доступного программного обеспечения.

Развитие компьютерных сетей, интеграция локальных сетей в одну общую сеть приводят к росту происшествий и атак. Для защиты от атак человечество придумывает все новые механизмы, и в то же самое время хакерские атаки становятся все более и более изощренными.

Одним из способов противодействия хакерским атакам является проведение процедуры аудита информационной безопасности, что позволяет на раннем этапе предотвращать атаки, искореняя причину их успешной реализации — обнаруживая и исправляя уязвимости компьютерных систем.

Цель пособия — дать возможность читателям на практических примерах изучить способы проведения одного из важнейших этапов аудита безопасности — инструментальных проверок защищенности компьютерных систем.

По мере изложения теоретического материала читателям предлагаются практические задания, обозначенные абзацем «**Выполнить!**». Выполнение заданий, а также получение ответов на содержащиеся в них вопросы являются необходимым условием освоения учебного материала. В процессе выполнения заданий в ряде случаев необходимо обеспечить функционирование в сети нескольких узлов, что зачастую бывает сложно организовать в компьютерных классах и невозможно на отдельно стоящем компьютере. Для изучения предлагается применять систему виртуальных машин VMware Workstation, позволяющую на одном компьютере имитировать наличие нескольких сетевых узлов.

Ознакомившись с теоретической частью пособия и выполнив практические задания, читатели смогут, во-первых, обоснованно применять методы сетевой защиты в процессе своей практической деятельности, во-вторых, самостоятельно освоить те средства и системы, которые остались за рамками данного пособия.

При проведении практических занятий применяются либо свободно распространяемые программные продукты, либо демонстрационные версии коммерческих систем.

Демонстрируются средства, позволяющие не только найти уязвимые места в настройке сетевых узлов, но и предложить конкретные меры по их устранению. Кроме того, с целью противодействия подобному сканированию, осуществляемому извне и несанкционированно, описываются приемы, которые используют сканеры безопасности для анализа уязвимостей.

Пособие состоит из трех глав и библиографического списка.

Глава 1. Понятие аудита информационной безопасности. В главе вводится понятие аудита информационной безопасности и трех его основных типов.

Глава 2. Методика проведения инструментальных проверок. Предложена и изложена оригинальная методика проведения важнейшего этапа аудита информационной безопасности. В результате выполнения практических заданий читатели получают навыки проведения инструментальных проверок. Читателям предлагается провести весь комплекс инструментальных проверок — от получения первичной информации о сетевых узлах до написания итогового отчета по результатам тестирования. В главе использованы материалы, подготовленные с участием В.В. Богданова.

Глава 3. Поиск уязвимостей Web-приложений. Предложен курс занятий, по результатам которых читатели изучат основные уязвимости, которые актуальны для многих современных серверов. Основная задача, преследуемая в данной части пособия, — научить читателей, многие из которых сталкиваются с безопасностью Интернет-сайтов и сами участвуют в их разработке, методике «ручного» выявления уязвимостей Web-приложений.

В качестве основы пособия использовались материалы курсов, читаемых авторами в Уральском федеральном университете имени первого Президента России Б. Н. Ельцина.

Библиографический список содержит 20 наименований источников, включая техническую документацию и учебные пособия, требующиеся для углубленного изучения отдельных тем.

1 ПОНЯТИЕ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аудит информационной безопасности (ИБ) представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области безопасности КС и вызывает постоянный интерес специалистов. Его основная задача — объективно оценить текущее состояние ИБ организации, а также ее адекватность поставленным целям и задачам бизнеса.

Под аудитом ИБ понимается системный процесс получения объективных качественных и численных оценок текущего состояния ИБ организации в соответствии с определенными критериями и показателями на всех основных уровнях обеспечения безопасности: нормативно-методологическом, организационно-управленческом, процедурном и программно-техническом [1].

Результаты квалифицированно выполненного аудита ИБ организации позволяют построить оптимальную по эффективности и затратам систему обеспечения информационной безопасности (СОИБ), представляющую собой комплекс технических средств, а также процедурных, организационных и правовых мер, объединенных на основе модели управления ИБ. В результате проведения аудита могут быть получены как качественные, так и численные оценки. При качественном оценивании, например, может быть приведен перечень уязвимостей в программно-аппаратном обеспечении с их классификацией по трехуровневой шкале опасности: высокая, средняя и низкая. Количественные оценки чаще всего применяются при оценке риска для активов организации, создаваемого угрозами безопасности. В качестве численных оценок могут выступать, например, цена риска, вероятность риска, размер риска и т. п.

Объективность аудита обеспечивается, в частности, тем, что оценка состояния ИБ производится специалистами на основе определенной методики, позволяющей объективно проанализировать все составляющие СОИБ.

Аудит ИБ может представлять собой услугу, которую предлагают специализированные фирмы, тем не менее в организации должен

проводиться внутренний аудит ИБ, выполняемый, например, администраторами безопасности.

1.1. Типы аудита информационной безопасности

Традиционно выделяют три типа аудита ИБ, которые различаются перечнем анализируемых компонентов СОИБ и получаемыми результатами:

- активный аудит;
- экспертный аудит;
- аудит на соответствие стандартам ИБ.

1.1.1. Активный аудит

Активный аудит представляет собой обследование состояния защищенности определенных подсистем информационной безопасности (ПИБ), относящихся к программно-техническому уровню. Например, вариант активного аудита, называемый тестом на проникновение (Penetration test), предполагает обследование подсистемы защиты сетевых взаимодействий.

Активный аудит включает:

- анализ текущей архитектуры и настроек элементов ПИБ;
- интервьюирование ответственных и заинтересованных лиц;
- проведение инструментальных проверок, охватывающих определенные ПИБ.

Анализ архитектуры и настроек элементов ПИБ проводится специалистами, обладающими знаниями по конкретным подсистемам, представленным в обследуемой системе (например, могут требоваться специалисты по активному сетевому оборудованию фирмы Cisco или по ОС семейства Microsoft), а также системными аналитиками, которые выявляют возможные изъяны в организации подсистем. Результатом этого анализа является набор опросных листов и инструментальных тестов.

Опросные листы используются в процессе интервьюирования лиц, отвечающих за администрирование АИС, для получения субъективных характеристик АИС, для уточнения полученных исходных данных и для идентификации некоторых мер, реализованных в рамках СОИБ. Например, опросные листы могут включать вопросы, связанные с политикой смены и назначения паролей, жизненным циклом АИС и степенью критичности отдельных ее подсистем для АИС и бизнес-процессов организации в целом.

Параллельно с интервьюированием проводятся инструментальные проверки (тесты), которые могут включать следующие мероприятия:

- визуальный осмотр помещений, обследование системы контроля доступа в помещения;
- получение конфигураций и версий устройств и ПО;
- проверка соответствия реальных конфигураций предоставленным исходным данным;
- получение карты сети специализированным ПО;
- использование сканеров защищенности (как универсальных, так и специализированных);
- моделирование атак, использующих уязвимости системы;
- проверка наличия реакции на действия, выявляемые механизмами обнаружения и реагирования на атаки.

Аудитор может исходить из следующих моделей, описывающих степень его знания исследуемой АИС (модель знания):

- модель «черного ящика» — аудитор не обладает никакими априорными знаниями об исследуемой АИС. Например, при проведении внешнего активного аудита (т. е. в ситуации, когда моделируются действия злоумышленника, находящегося вне исследуемой сети), аудитор может, зная только имя или IP-адрес Web-сервера, пытаться найти уязвимости в его защите;
- модель «белого ящика» — аудитор обладает полным знанием о структуре исследуемой сети. Например, аудитор может обладать картами и диаграммами сегментов исследуемой сети, списками ОС и приложений. Применение данной модели не в полной мере имитирует реальные действия злоумышленника, но позволяет, тем не менее, представить «худший» сценарий, когда атакующий обладает полным знанием о сети. Кроме того, это позволяет построить сценарий активного аудита таким образом, чтобы инструментальные тесты имели минимальные последствия для АИС и не нарушали ее нормальной работы;
- модель «серого ящика», или «хрустального ящика» — аудитор имитирует действия внутреннего пользователя АИС, обладающего учетной записью доступа в сеть с определенным уровнем полномочий. Данная модель позволяет оценить риски, связанные с внутренними угрозами, например, от неблагонадежных сотрудников компании.

Аудиторы должны согласовывать каждый тест, модель знания, применяемую в тесте, и возможные негативные последствия теста с

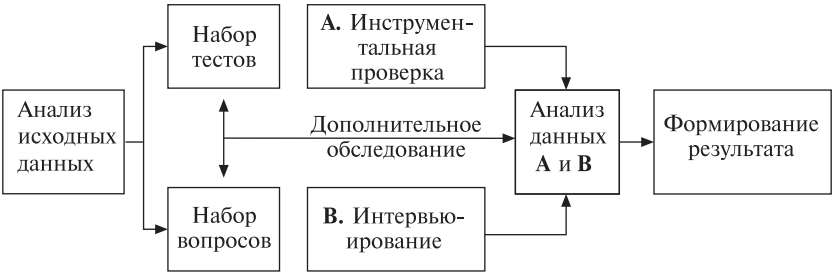

Рис. 1.1. Схема проведения активного аудита ИБ

лицами, заинтересованными в непрерывной работе АИС (руководителями, администраторами системы и др.).

По результатам инструментальной проверки проводится пересмотр результатов предварительного анализа и, возможно, организуется дополнительное обследование (рис. 1.1).

По результатам активного аудита создается аналитический отчет, состоящий из описания текущего состояния технической части СОИБ, списка найденных уязвимостей АИС со степенью их критичности и результатов упрощенной оценки рисков, включающей модель нарушителя и модель угроз. Дополнительно может быть разработан план работ по модернизации технической части СОИБ, состоящий из перечня рекомендаций по обработке рисков.

1.1.2. Экспертный аудит

Экспертный аудит предназначен для оценивания текущего состояния ИБ на нормативно-методологическом, организационно-управленческом и процедурном уровнях. Экспертный аудит проводится преимущественно внешними аудиторами, его выполняют силами специалистов по системному управлению. Сотрудники организации-аудитора совместно с представителями заказчика проводят следующие виды работ:

- сбор исходных данных об АИС, ее функциях и особенностях, используемых технологиях автоматизированной обработки и передачи информации;
- сбор информации об имеющихся организационно-распорядительных документах по обеспечению ИБ и их анализ;
- определение защищаемых активов, ролей и процессов СОИБ.

Важнейшим инструментом экспертной оценки является сбор данных об АИС путем интервьюирования технических специалистов и руководства заказчика.

Основные цели интервьюирования руководящего состава организации:

- определение политики и стратегии руководства в вопросах обеспечения ИБ;
- выявление целей, которые ставятся перед СОИБ;
- выяснение требований, которые предъявляются к СОИБ;
- получение оценок критичности тех или иных подсистем обработки информации, оценок финансовых потерь при возникновении тех или иных инцидентов.

Основные цели интервьюирования технических специалистов:

- сбор информации о функционировании АИС;
- получение схемы информационных потоков в АИС;
- получение информации о технической части СОИБ;
- оценка эффективности работы СОИБ.

В рамках экспертного аудита проводится анализ организационно-распорядительных документов, таких как политика безопасности, план защиты, различного рода положения и инструкции. Организационно-распорядительные документы оцениваются на предмет достаточности и непротиворечивости декларируемым целям и мерам ИБ, а также на предмет соответствия стратегической политике руководства в вопросах ИБ.

Результаты экспертного аудита могут содержать рекомендации по совершенствованию нормативно-методологических, организационно-управленческих и процедурных компонентов СОИБ.

1.1.3. Аудит на соответствие стандартам ИБ

В ряде случаев проводится аудит на соответствие стандартам ИБ. Специально уполномоченные организации-аудиторы по результатам аудита принимают решение и выдают документальное подтверждение о соответствии СОИБ тому или иному эталонному стандарту (проводят сертификацию). Сертификация является показателем качества СОИБ и поднимает престиж и уровень доверия к организации.

Аудит на соответствие стандартам чаще всего подразумевает проведение активного и экспертного аудита. По результатам могут быть подготовлены отчеты, содержащие следующую информацию:

- степень соответствия проверяемой ИС выбранным стандартам;
- число и категории полученных несоответствий и замечаний;
- рекомендации по построению или модификации СОИБ, позволяющие привести ее в соответствие с требованиями рассматриваемого стандарта.

1.2. Методология проведения аудита информационной безопасности в национальных и отраслевых стандартах

Методология проведения аудита ИБ сформулирована, в частности, в таких документах, как [4–10].

Документы [4–6] конкретизируют методику для информационных систем банковской сферы Российской Федерации. Здесь понятие аудита информационной безопасности организации банковской системы Российской Федерации определяется как периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в организациях банковской сферы РФ установленных требований по обеспечению информационной безопасности. Предполагается два вида аудита: внутренний и внешний. Внутренний аудит проводятся самой организацией или от ее имени для анализа менеджмента или других внутренних целей и могут служить основанием для самодекларации организации о соответствии требованиям по ИБ. Внешний аудит проводится сторонами, заинтересованными в деятельности организации, например потребителями или другими лицами от их имени, а также внешними независимыми организациями. Указывается, что работы по проведению аудита ИБ должны включать следующие этапы:

- подготовка к проведению аудита ИБ;
- анализ документов;
- проведение аудита ИБ на месте;
- подготовка, утверждение и рассылка отчета по аудиту ИБ;
- завершение аудита ИБ.

Основными источниками свидетельств аудита ИБ должны являться:

- документы проверяемой организации и третьих лиц, относящиеся к обеспечению ИБ организации;
- устные высказывания и письменные ответы сотрудников проверяемой организации в процессе проводимых опросов;
- результаты наблюдений аудиторов за деятельностью организации в области ИБ.

Основными методами получения свидетельств аудита ИБ являются:

- проверка и анализ документов, касающихся обеспечения ИБ организации;
- наблюдение за деятельностью организации в области ИБ;