# НАУЧНАЯ СТАТЬЯ: «АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ АО «СОФТЛАЙТ ТРЕЙД»

**Аннотация: в** статье рассматриваются сущность и значение аудита информационной безопасности предприятия, проанализированы сильные и слабые стороны в развитии организации, разработаны рекомендации, направленные на повышение эффективности аудита информационной безопасности предприятия.

**Ключевые слова:** аудит, информационная безопасность.

Сегодня информационные системы (ИС) играют ключевую роль в обеспечении эффективности работы коммерческих и государственных предприятий. Повсеместное использование ИС для хранения, обработки и передачи информации делает актуальными проблемы их защиты, особенно учитывая глобальную тенденцию к росту числа информационных атак, приводящих к значительным финансовым и материальным потерям. Для эффективной защиты от атак компаниям необходима объективная оценка уровня безопасности ИС - именно для этих целей и применяется аудит безопасности.

Определение аудита безопасности еще не устоялось, но в общем случае его можно описать как процесс сбора и анализа информации об ИС для качественной или количественной оценки уровня ее защищенности от атак злоумышленников. Существует множество случаев, когда целесообразно проводить аудит безопасности. Это делается, в частности, при подготовке технического задания на проектирование и разработку системы защиты информации и после внедрения системы безопасности для оценки уровня ее эффективности. Возможен аудит, направленный на приведение действующей системы безопасности в соответствие требованиям российского или международного законодательства. Аудит может также предназначаться для систематизации и упорядочения существующих мер защиты информации или для расследования произошедшего инцидента, связанного с нарушением информационной безопасности.

Как правило, для проведения аудита привлекаются внешние компании, которые предоставляют консалтинговые услуги в области информационной безопасности. Инициатором процедуры аудита может стать руководство предприятия, служба автоматизации или служба информационной безопасности. В ряде случаев аудит также проводится по требованию страховых компаний или регулирующих органов. Аудит безопасности выполняется группой экспертов, численность и состав которой зависит от целей и задач обследования, а также от сложности объекта оценки.

Можно выделить следующие основные виды аудита информационной безопасности:

экспертный аудит безопасности, в ходе которого выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в процедуре обследования;

оценка соответствия рекомендациям международного стандарта ISO 17799, а также требованиям руководящих документов ФСТЭК (Гостехкомиссии);

инструментальный анализ защищенности ИС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы;

комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования.

Любой из перечисленных видов аудита может проводиться по отдельности или в комплексе, в зависимости от тех задач, которые решает предприятие. В качестве объекта аудита может выступать как ИС компании в целом, так и ее отдельные сегменты, в которых обрабатывается информация, подлежащая защите.

Проведение аудита безопасности

В общем случае аудит безопасности, вне зависимости от формы его проведения, состоит из четырех основных этапов, на каждом из которых выполняется определенный круг работ (см. рисунок 1).

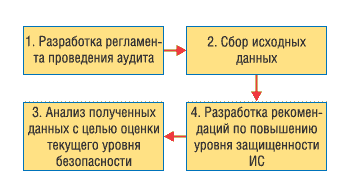


Рисунок 1 - Этапы аудита информационной безопасности

Проведенный аудит информационной безопасности АО «СофтЛайн Трейд» выявил следующее:

Помещения компании находятся на втором этаже бизнес-центра. Компания занимает несколько комнат на одном этаже.

При описании результатов аудита информационной системы были приняты следующие обозначения помещений офиса компании:

комната 1 - подразделение «Бизнес»;

комната 2 - подразделение «Политика»;

комната 3 - переговорная комната;

комната 4 – reception;

комната 5 - серверная комната

**Локальная сеть**

**Топология сети**

Во всех помещениях имеется разводка кабелей типа RJ45 в соответствующие розетки. Все кабели заведены в серверную комнату, коммутационные панели (патч-панели) отсутствуют. Все кабели обжаты разъемами и подключены непосредственно к активному оборудованию. В настоящее время расширение или модификации кабельной сети не планируется. Претензий к качеству кабельной системы не имеется.

**Используемое активное сетевое оборудование**

В компании используется разное сетевое оборудование. Полный перечень используемого оборудования приведен в Таблице 1.

Таблица 1

|  |  |  |
| --- | --- | --- |
| Помещение | Оборудование | Назначение оборудования |
| Комната 5 | Маршрутизатор Cisco 1800 | Подключение к Интернет |
| Коммутатор Compex SAS 2224 | Подключение рабочих мест пользователей |
| Коммутатор D-Link DES-1024D | Подключение рабочих мест пользователей |
| АТС Panasonic TA-616RU, 2 модуля | Офисная телефонная станция |
| Комната 3 | Точка беспроводного доступа (Wi-Fi) D-Link | Обеспечение беспроводного доступа к локальной сети |

**Состав и состояние пассивных компонентов локальной сети**

В основном состояние удовлетворительное. У компании нет претензий по работоспособности кабельной системы.

**Вид и форма получения внешних сервисов**

Доступ в Интернет предоставляет провайдер DVKNET (www.dvknet.ru). Подключение организовано по кабелю «витая пара» RJ45, скорость 1.5 Мбит/сек, тариф безлимитный. Внешний IP адрес ХХ.ХХХ.ХХХ.ХХ (ХХХХХХ.dvknet.ru). Интернет подключен через маршрутизатор Cisco 1800. Управление маршрутизатором осуществляет провайдер, хотя само устройство принадлежит компании «Софтлайн Трейд». В число внешних сервисов также входит хостинг электронной почты, предоставляемый компанией РБК. Удаленного доступа для управления локальной сетью из Интернета нет.

# Центральная точка (ЦТ)

Центральная точка расположена в комнате 5, которая представляет собой запираемое помещение размером 1 на 1,5 метра. Систем вентиляции и кондиционирования нет. Коммуникационная стойка или шкаф отсутствуют. Все оборудование размещено на металлических стеллажах. В состав центральной точки входит :

- Маршрутизатор Cisco 1800, подключено 1 порт WAN и 1 порт LAN;

- Коммутатор Compex SAS2224 на 24 порта, из них занято 19 портов;

- Коммутатор D-Link DES-1024D на 24 порта, все порты заняты;

- Сервер PS1

- Сервер PS2

- 3 источника бесперебойного питания PowerCOM мощностью 1300 VA каждый.

Сервер PS1 играет роль файлового сервера и домен контроллера. На сервере установлена серверная операционная система Windows 2003 Server Enterprise. Сервер представляет собой обычный компьютер, собранный самостоятельно. Характеристики сервера представлены в таблице 2:

Таблица 2.

|  |  |  |  |
| --- | --- | --- | --- |
| Процессор | Память | Оптический привод | Жесткие диски  (все диски IDE, RAID массивы или зеркалирование не используется) |
| Pentium 4 1,8 GHz | 256 Мб | DVD-RW | Диск 0 – 40 Гб, разбит на  С: (7Гб, 1,8 свободно) - Система  D: (33 Гб, 6,4 свободно) – Архив |
|  |  |  | Диск 1 – 40 Гб,  G: - Резервный, 221 Мб свободно |
|  |  |  | Диск 2 – 120 Гб, разбит на  F: (60 Гб, 20 свободно) – Бэкап и  E: (60 Гб, 4,8 свободно) – ХХХХХ.  На диске E хранятся файлы пользователей |

На сервере установлено антивирусное программное обеспечение Symantec версии 10 и консоль управления. Резервное копирование данных выполняется с помощью программы Acronis True Image с понедельника по пятницу. Образы создаются на дисках F: и D:. Помимо этого, создается бэкап System State также с понедельника по пятницу.

Для управления ресурсами сети используется технология Активная Директория (AD) Microsoft. Характеристики AD приведены ниже:

- Количество учетных записей пользователей – 19;

- Количество учетных записей компьютеров – 16;

- Количество домен контроллеров – 1;

- Количество подразделений – 9;

- Количество объектов групповой политики – 8 (включая стандартные);

- Размер базы данных AD – 31 Мб.

На сервере PS1 также работает служба DHCP для выделения IP адресов в подсети 10.10.10.x, а также DNS сервер для поддержки AD.

Сервер PS2 играет роль почтового сервера и сервера службы обновлений WSUS. Установлена серверная операционная система Windows 2003 Server Enterprise. Почтовый сервер работает под управлением программы Microsoft Exchange 2003. При этом почтовая функциональность внутри компании не используется, а используются только возможности совместной работы в MS Exchange, такие как, доступ к календарям, задачам и т.д. Общие папки для хранения документов также не используются. Сервер представляет собой обычный компьютер, собранный самостоятельно. Характеристики сервера представлены в таблице 3.

Таблица 3.

|  |  |  |  |
| --- | --- | --- | --- |
| Процессор | Память | Оптический привод | (все диски IDE, RAID массивы или зеркалирование не используется) |
| AMD Sempron 2400+ 1,6 GHz | 512 Мб | DVD-RW | Диск 0 – 150 Гб, разбит на  С: (113 Гб, 83 свободно) - Система  D: (36 Гб, 20 свободно) – Рабочий |
|  |  |  | Диск 1 – 40 Гб,  E: - Backup, 12Гб свободно |

Характеристики почтового хранилища MS Exchange:

- количество почтовых ящиков – 8;

- размер самого большого ящика – 681 Мб;

- размер базы почтовых ящиков – 8 Гб;

- размер базы общих папок – 42 Мб;

Размер хранилища службы обновлений – 6, 26 Гб.

На сервере PS2 имеется DNS сервер для поддержки службы AD, а также Microsoft SQL Server 2000 для поддержки службы обновлений.

На сервере также установлено антивирусное программное обеспечение Symantec версии 10 и консоль управления. Резервное копирование выполняется с помощью Acronis True Image по воскресеньям на диск E:. Резервное копирование почтового хранилища Exchange отдельно не делается.

# Пользовательские места

**Количество и распределение рабочих мест (существующих и планируемых)**

Рабочие места имеются в комнатах 1, 2 и 4. В комнате 1 имеется больше рабочих мест, чем используется компанией «СОФТЛАЙН ТРЕЙД». Некоторые рабочие места используются сотрудниками другой компании просто для выхода в Интернет. Сотрудники другой компании не пользуются ресурсами внутренней сети компании «СОФТЛАЙН ТРЕЙД» и работают в своей рабочей группе.

Распределение рабочих мест сотрудников по помещениям приведено в Таблице 4.

Таблица 4

|  |  |  |
| --- | --- | --- |
| Помещение | Используется рабочих мест | Планируется использовать рабочих мест |
| Комната 1 | 6 |  |
| Комната 2 | 7 |  |
| Комната 3 | Точка беспроводного доступа |  |
| Комната 4 | 1 |  |

**Перечень оборудования и программного обеспечения, установленного на рабочих местах пользователей.**

Подробное описание конфигураций компьютеров пользователей и установленного на него основного программного обеспечения приведено в Таблице 5.

Все рабочие места оснащены источниками бесперебойного питания APC Back UPS мощностью 500VA или 350VA.

Оборудование рабочих мест пользователей выполнялось по мере возникновения необходимости в них. Система в приобретении компьютерной техники отсутствует. В результате имеется парк достаточно разнообразной компьютерной техники. Гарантийные сроки на оборудование закончились. Все компьютеры самостоятельной сборки (noname). Основные жалобы пользователей – на невысокое быстродействие. Сетевые устройства, видеоконтроллеры и аудиоконтроллеры, установленные в настольных компьютерах удовлетворяют требованиям офисной работы и их подробное описание не приводится.

Мониторы на 80% рабочих мест удовлетворяют требованиям офисной работы.

Программное обеспечение разнообразное. Отсутствует единый стандарт на основные продукты (операционная система и пакет офисных программ). Все программное обеспечение на рабочих местах лицензиями не подкреплено. Процесса централизованного обновления программного обеспечения не существует.