программно-технических механизмов защиты может быть сведена к нулю в случае, если пользователи информационных систем игнорируют элементарные правила парольной политики. Установка межсетевого экрана может даже понизить защищенность сети в случае отсутствия политики управления доступом, которую он должен реализовывать. В основе организационных мер защиты информации лежат политики безопасности организации, от эффективности которых в наибольшей степени зависит успешность мероприятий по обеспечению ИБ.

Важно помнить, что прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия.

**Литература:**

1. *Разработка политики информационной безопасности предприятия*. Сергей Петренко, Владимир Курбатов, компания АйТи.
2. *Разработка правил информационной безопасности*. Скотт Бармен.
3. *Практические аспекты разработки политики информационной безопасности*. Сергей А. Охрименко, Константин Ф. Склифос.
4. *Формирование политики безопасности для информационной системы*. Сергей А. Охрименко, Геннадий А. Черней.
5. *Политика безопасности: разработка и реализация*. В.Г. Грибунин.
6. Основные положения международного стандарта безопасности ISO/IEC 17799.

***Анна Милованова,***
*«IT&IS Management»*

# АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На сегодняшний день корпоративные сети даже небольших компаний представляют собой достаточно сложные и многофункциональные объекты, позволяющие решать различные задачи. Нынешняя тенденция к усложнению функциональности, администрирования информационных систем ведет к появлению возрастающего числа ошибок, связанных с безопасностью системы, а иногда к недостаточности опыта и знаний для безопасного администрирования системы.

В связи с этим общепринятой практикой является проведение сторонней, доверенной, специализированной компанией всестороннего аудита информационной безопасности (ИБ) всех автоматизированных ресурсов и бизнес-процессов компании.

Аудит ИБ представляет собой комплекс мероприятий получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности в компании, проводимый независимыми экспертами в соответствии с бизнес-процессами компании и международными стандартами. Объектами аудита могут выступать как информационная система в целом, так и ее отдельные компоненты, обеспечивающие обработку конфиденциальной информации.

Аудит ИБ позволяет установить соответствие уровня ИБ компании выдвигаемым внутренним требованиям, требованиям действующего законодательства и международных стандартов, а также степень обеспечения параметров конфиденциальности, целостности и доступности ресурсов информационной системы.

Аудит ИБ можно разделить на два основных вида:

- экспертный аудит – выявление недостатков в системе защиты информации на основе опыта экспертов, участвующих в аудите;
- аудит на соответствие международным стандартам – сравнение состояния ИБ компании с неким абстрактным описанием, приводимым в международных стандартах.

Среди основных стандартов, на соответствие которым проводится аудит ИБ, можно выделить:

- ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- ISO/IEC 17799:2005 Информационная технология. Практические правила управления информационной безопасностью.

Следует отметить, что для организации оптимального подхода к проведению аудита ИБ следует использовать и совершенствовать идею активного аудита ИБ, суть которой заключается в сочетании теста на проникновение и аудита ИБ в традиционном понимании. В процессе аудита ИБ в основном применяют следующие методики:

- методика активного комплексного аудита, включая обязательные тесты на проникновение как из внешней, так и из внутренней сети;
- методика КОНДОР основана на проверке соответствия требованиям стандартов ISO/IEC 27-001:2005 и ISO/IEC 17799:2005;
- методика ГРИФ основана на модели угрозы – уязвимости для определения рисков безопасности.

На основе сложившейся практики при проведении аудита ИБ рекомендуется основываться на следующих принципах [4]:

- применение моделей нарушителей как внутреннего нарушителя (например, инсайдер), так и внешнего нарушителя (например, хакер, компьютерный преступник);
- определение области проведения аудита;
- анализ путей повышения привилегий – аудитор изначально

имеет только физический доступ к обследуемой информационной системе, логические права доступа ему не предоставляются, после чего аудитор отрабатывает все возможные пути повышения привилегий от «нулевого» уровня, оценивая критичность и вероятность их реализации;
- анализ влияния выявленных уязвимостей на защищенность всей информационной системы в целом;
- поиск новых уязвимостей;
- наличие строгой системы классификации уязвимостей;
- применение методов социальной инженерии для имитации действий нарушителя, направленных на пользователей информационной системы.

В число задач, которые решаются в ходе проведения аудита ИБ, входят:
- сбор и анализ исходных данных об организационной и функциональной структуре информационной системы;
- анализ существующей политики обеспечения ИБ на предмет полноты и эффективности;
- выявление значимых угроз ИБ и путей их реализации;
- выявление и ранжирование по степени опасности существующих уязвимостей технологического и организационного характера в информационной системе;
- анализ информационных и технологических рисков, связанных с осуществлением угроз ИБ через выявленные уязвимости;
- проведение тестовых сценариев по нарушению ИБ критически важных компонентов информационной системы;
- разработка предложений и рекомендаций по политике обеспечения ИБ, по внедрению новых и повышению эффективности существующих механизмов обеспечения ИБ.

Результатом проведенного аудита является детальный отчет, содержащий описание всех выявленных технологических уязвимостей обследуемой информационной системы, комплексную оценку системы управления ИБ, а также разработанные рекомендации по повышению текущего уровня обеспечения ИБ.

Можно отметить, что одним из критериев качества выполненного аудита является полнота выявленных недостатков, уязвимостей и несоответствий в системе обеспечения безопасности компании и содержательность рекомендаций по их устранению.

Результаты проведенного исследования в Республике Молдова [3] показывают, что из числа опрошенных компаний лишь в 30% проводился аудит ИБ, в 40% не проводился, в 6,7% планируется, а в 18,3% даже не планируется. Большинство респондентов считают, что уровень ИБ их компаний недостаточен, что доказывает необходимость в проведении аудитов ИБ с точки зрения уменьшения рисков и улучшения процессов. Однако 11,5% компаний намерены снижать финансирование про-

грамм в области ИБ, в противовес им 77% наоборот намерены увеличивать затраты.

Несмотря на это, следует отметить, что многие компании будут заинтересованы в аудите ИБ, так как зачастую руководству компаний требуется независимая оценка состояния ИБ, деятельности служб ИБ и проектов в данной области.

**Список нормативной и научной литературы:**

1. ISO/IEC 17799:2005 Информационная технология. Практические правила управления информационной безопасностью.
2. ISO/IEC 27000 – Семейство Международных Стандартов Управления Информационной Безопасностью.
3. www.crime-research.md.
4. www.itsec.ru.

***Лилия Павлова,***
*компания IT&IS Management SRL*

# УПРАВЛЕНИЕ РИСКАМИ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

В настоящее время информационные технологии (ИТ) значительно расширили возможности для ведения бизнеса. Высокие технологии позволяют не только повысить эффективность бизнес-процессов, но и могут стать источником колоссального ущерба. Утечка конфиденциальных данных, вирусы, хакеры, спам – данных проблем почти невозможно избежать, так как их существование обусловлено применением ИТ в бизнесе. Тем не менее, ИТ-рисками можно управлять.

Управление ИТ-рисками становится все более значимым разделом общей системы Управления Рисками. Меры по анализу и минимизации ИТ-рисков составляют предмет отдельной дисциплины – управление информационно-технологическими рисками (Information Technology Risk Management – ITRM).

Управление ИТ-рисками состоит из их периодической оценки и выполнения мероприятий по снижению выявленных рисков до приемлемого уровня. Данный процесс включает в себя управление рисками безопасности, доступности, производительности и согласованности.

Для управления ИТ-рисками необходимо применять:

- методики, учитывающие положения и требования международных стандартов ISO/IEC 17799, BS7799, ISO/IEC 27001;
- CobiT (Control Objectives for Information and related Technology);
- рекомендации NIST (National Institute of Standards and Tech-