УДК 004.056

АУДИТ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Аскарбеков Б. А., Исирапилов К. Э.
Кыргызский государственный университет строительства, транспорта и архитектуры имени Н. Исанова

В статье дается определение аудита информационной безопасности. Описаны этапы проведения аудита информационной безопасности. Отмечено, что аудит проводится не по инициативе аудитора, а по инициативе руководства предприятия, которое в данном вопросе является основной заинтересованной стороной. Поддержка руководства предприятия является необходимым условием для проведения аудита.

***Ключевые слова*:** информационная безопасность, аудит информационной безопасности, информационные системы.

МААЛЫМАТТЫК ТУТУМДАРДЫН КООПСУЗДУК АУДИТИ

Аскарбеков Б. А., Исирапилов К. Э.
Н. Исанов атындагы Кыргыз мамлекеттик курулуш, транспорт жана архитектуры университети

Макалада маалыматтык коопсуздук аудитинин аныктамасы берилет. Маалыматтык коопсуздукка аудит жүргүзүүнүн этаптары баяндалган. Аудит аудитордун демилгеси менен эмес, ишкананын жетекчилигинин демилгеси менен ишке ашырылары жана ал бул маселе боюнча негизги кызыкдар тарап болуп саналары белгиленген. Компаниянын жетекчилиги тарабынан колдоо аудит жүргүзүү үчүн зарыл шарт болуп саналат.

***Баштапкы сөздөр*:** маалыматтык коопсуздук, маалыматтык коопсуздук аудити, маалыматтык системалар.

SECURITY AUDIT OF INFORMATION SYSTEMS

Askarbekov B. A., Isirapilov K. E.

Kyrgyz State University of Construction, Transport and Architecture named after N. Isanov

This article defines an information security audit. The stages of information security audit are described. It is noted that the audit is carried out not on the initiative of the auditor, but on the initiative of the management of the enterprise, which in this matter is the main interested party. Enterprise management support is a prerequisite for auditing.
Keywords: information security, information security audit, information systems.

Аудит представляет собой независимую экспертизу отдельных областей функционирования организации. Различают внешний и внутренний аудит. Внешний аудит — это, как правило, разовое мероприятие, проводимое по инициативе руководства организации или акционеров. Рекомендуется проводить внешний аудит регулярно, а, например, для многих финансовых организаций и акционерных обществ это является обязательным требованием со стороны их учредителей и акционеров. Внутренний аудит представляет собой непрерывную деятельность, которая осуществляется на основании «Положения о внутреннем аудите» и в соответствии с планом, подготовка которого осуществляется подразделениями службы безопасности и утверждается руководством организации.

Целями проведения аудита безопасности являются:

• анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов;

• оценка текущего уровня защищенности ИС;

• локализация узких мест в системе защиты ИС;

• оценка соответствия ИС существующим стандартам в области информационной безопасности;

• выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Аудит безопасности предприятия (фирмы, организации) должен рассматриваться как конфиденциальный инструмент управления, исключающий в целях конспирации возможность предоставления

информации о результатах его деятельности сторонним лицам и организациям.

Для проведения аудита безопасности предприятия может быть рекомендована следующая последовательность действий.

Подготовка к проведению аудита безопасности:

• выбор объекта аудита (фирма, отдельные здания и помещения, отдельные системы или их компоненты);

• составление команды аудиторов-экспертов;

• определение объема и масштаба аудита и установление конкретных сроков работы.

Проведение аудита:

• общий анализ состояния безопасности объекта аудита;

• регистрация, сбор и проверка статистических данных и результатов инструментальных измерений опасностей и угроз;

• оценка результатов проверки;

• составление отчета о результатах проверки по отдельным составляющим.

Завершение аудита:

• составление итогового отчета;

• разработка плана мероприятий по устранению узких мест и недостатков в обеспечении безопасности фирмы.

Для успешного проведения аудита безопасности необходимо:

• активное участие руководства фирмы в его проведении;

• объективность и независимость аудиторов (экспертов), их компетентность и высокая профессиональность;

• четко структурированная процедура проверки;

• активная реализация предложенных мер обеспечения и усиления безопасности.

Аудит безопасности, в свою очередь, является действенным инструментом оценки безопасности и управления рисками. Предотвращение

угроз безопасности означает в том числе и защиту экономических, социальных и информационных интересов предприятия.

В зависимости от объема анализируемых объектов предприятия определяются масштабы аудита:

• аудит безопасности всего предприятия в комплексе;

• аудит безопасности отдельных зданий и помещений (выделенные помещения);

• аудит оборудования и технических средств конкретных типов и видов;

• аудит отдельных видов и направлений деятельности: экономической, экологической, информационной, финансовой и т. д.

Следует подчеркнуть, что аудит проводится не по инициативе аудитора, а по инициативе руководства предприятия, которое в данном вопросе является основной заинтересованной стороной. Поддержка руководства предприятия является необходимым условием для проведения аудита.

Аудит представляет собой комплекс мероприятий, в которых помимо самого аудитора, оказываются задействованными представители большинства структурных подразделений компании. Действия всех участников этого процесса должны быть скоординированы. Поэтому на этапе инициирования процедуры аудита должны быть решены следующие организационные вопросы:

• права и обязанности аудитора должны быть четко определены и документально закреплены в его должностных инструкциях, а также в положении о внутреннем (внешнем) аудите;

• аудитором должен быть подготовлен и согласован с руководством 10 план проведения аудита;

• в положении о внутреннем аудите должно быть закреплено, в частности, что сотрудники предприятия обязаны оказывать содействие аудитору и предоставлять всю необходимую для проведения аудита информацию.

На этапе инициирования процедуры аудита должны быть определены границы проведения обследования. Если какие-то информационные подсистемы предприятия не являются достаточно критичными, их можно исключить из границ проведения обследования.

Другие подсистемы могут оказаться недоступными для аудита из-за соображений конфиденциальности.

Границы проведения обследования определяются в следующих категориях:

1. Список обследуемых физических, программных и информационных ресурсов.

2. Площадки (помещения), попадающие в границы обследования.

3. Основные виды угроз безопасности, рассматриваемые при проведении аудита.

4. Организационные (законодательные, административные и процедурные), физические, программно-технические и прочие аспекты обеспечения безопасности, которые необходимо учесть в ходе проведения обследования, и их приоритеты (в каком объеме они должны быть учтены).

План и границы проведения аудита обсуждается на рабочем собрании, в котором участвуют аудиторы, руководство компании и руководители структурных подразделений. Для понимания аудита ИБ как комплексной системы может быть использована его концептуальная модель. Здесь главные составляющие процесса:

- объект аудита;
- цель аудита;
- предъявляемые требования;
- используемые методы;
- масштаб:
- исполнители;
- порядок проведения.

С точки зрения организации работ при проведении аудита ИБ выделяют три принципиальных этапа:

1. сбор информации;

2. анализ данных;

3. выработка рекомендаций и подготовка отчетных документов.

Таким образом, проведение аудита информационной безопасности состоит из нескольких основных этапов:

• инициирование процедуры проверки (четкое определение прав и обязанностей аудитора, подготовка аудитором плана проверки и его согласование с руководством, решение вопроса о границах проведения исследования, накладывание на сотрудников организации обязательства в помощи и своевременном предоставлении необходимой информации);

• сбор исходных данных (структура системы безопасности, распределение средств обеспечения безопасности, уровни функционирования системы безопасности, анализ методов получения и предоставления информации, определение каналов связи и взаимодействия ИС с другими структурами, иерархия пользователей компьютерных сетей, определение протоколов и т.д.);

• проведение комплексной или частичной проверки; анализ полученных данных (анализ рисков любого типа и соответствия стандартам);

• выдача рекомендаций по устранению возможных проблем;

• создание отчетной документации.

Первый этап является наиболее простым, поскольку его решение принимается исключительно между руководством предприятия и аудитором. Границы проведения анализа могут быть рассмотрены на общем собрании сотрудников или акционеров. Все это в большей степени относится к правовому полю.

Второй этап сбора исходных данных, будь то проведение внутреннего аудита информационной безопасности или внешней независимой аттестации, является наиболее ресурсоемким. Связано это с тем, что на этой

стадии нужно не только изучить техническую документацию, касающуюся всего программно-аппаратного комплекса, но и провести узконаправленное интервьюирование сотрудников компании, причем в большинстве случаев даже с заполнением специальных опросных листов или анкет.

Что же касается технической документации, здесь важно получить данные о структуре ИС и приоритетных уровнях прав доступа к ней сотрудников, определить общесистемное и прикладное программное обеспечение (используемые операционные системы, приложения для ведения бизнеса, управления им и учета), а также установленные средства защиты софтверного и непрограммного типа (антивирусы, файрволлы и т.д.). Кроме того, сюда включается полная проверка сетей и провайдеров, предоставляющих услуги связи (организация сети, используемые протоколы для подключения, типы каналов связи, методы передачи и приема информационных потоков и многое другое). Как уже понятно, это занимает достаточно много времени.

На следующем этапе определяются методы аудита информационной безопасности. Их различают три:

• анализ рисков (самая сложная методика, базирующаяся на определении аудитором возможности проникновения в ИС и нарушения ее целостности с применением всех возможных методов и средств);

• оценка соответствия стандартам и законодательным актам (наиболее простой и самый практичный метод, основанный на сравнении текущего состояния дел и требований международных стандартов и внутригосударственных документов в сфере информационной безопасности);

• комбинированный метод, объединяющий два первых.

После получения результатов проверки начинается их анализ. Средства аудита информационной безопасности, которые применяются для анализа, могут быть достаточно разнообразными. Все зависит от специфики

деятельности предприятия, типа информации, используемого программного обеспечения, средств защиты и пр.

На основе проведенного анализа эксперт делает заключение о состоянии защиты и выдает рекомендации по устранению имеющихся или возможных проблем, модернизации системы безопасности и т.д. При этом рекомендации должны быть не только объективными, но и четко привязанными к реалиям специфики предприятия. Иными словами, советы по апгрейду конфигурации компьютеров или программного обеспечения не принимаются. В равной степени это относится и к советам по увольнению «ненадежных» сотрудников, установке новых систем слежения без конкретного указания их назначения, места установки и целесообразности.

В заключении можно отметить, что результаты проведения аудита ИБ позволяют выявить значимые угрозы для информации, оценить вероятность каждого события, представляющего угрозу для безопасности, и ущерб от него, а также оценить с точки зрения этих требований эффективность применяемых организационных мер и инженерно-технических средств защиты.

ЛИТЕРАТУРА

1. Аверченков, В.И. Аудит информационной безопасности: учеб. пособие для вузов / В.И. Аверченков. – 2-е изд., стер. – Брянск: БГТУ, 2010.–268 с.
2. Курило А.П. Аудит информационной безопасности. - БДЦ-пресс, 304 стр. 2006 г.