УДК 004.056.5

Больбат Е.П.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

ФГБОУ ВПО «Амурский гуманитарно-педагогический
государственный университет»
г. Комсомольск-на-Амуре, Россия,
rei_kosandro@mail.ru

Для современных предприятий автоматизация бизнес-процессов с использованием средств вычислительной техники и телекоммуникаций являются той неотъемлемой частью их развития. В обеспечении эффективности работы коммерческих и государственных предприятий ключевую роль играют информационные системы (ИС). Это определяется неуклонным ростом информации, которая является одним из ключевых ресурсов любой организации, от которого напрямую зависит успешность и прибыльность предприятий.

За счет использование ИС для хранения, обработки и передачи информации, а также бесконтрольное использование Интернет, переносных носителей, отсутствия мониторинга печатающейся информации на принтерах, увеличиваются шансы кражи особо важной информации предприятий. Самые распространяемые причины кражи информации особо важной для предприятий являются: конкуренция либо возможность наживы. Как нам известно, любая ИС в процессе своей работы эволюционирует и видоизменяется. В некоторых случаях может возникнуть ситуация, в которой система еще работает, но неизвестно, что произойдет в случае возникновения угрозы безопасности. В данном случае для эффективности защиты требуется объективная оценка уровня безопасности ИС.

Решением этой проблемы является аудит информационной безопасности (ИБ). Определение аудита безопасности конкретизировано не устоялось, но

исходя из различных источников, его можно описать как процесс сбора и анализа об ИС для качественной или количественной оценки уровня ее защищенности от атак злоумышленников. Иными словами это всесторонние обследование, задачей которого является оценка текущее состояние ИБ, а результатом - построение эффективной системы защиты, которая будет соответствовать текущим целям и задачам, как предприятий, так и отдельных критичных областей ИС [1,3].

Целями аудита ИБ является:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
- оценка текущего уровня защищенности ИС;
- оценка соответствия ИС существующим стандартам в области ИБ и политике безопасности организации;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС [2].

Можно выделить основные виды аудита ИБ:

- 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 ISQ 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 [1].

Для проведения аудита ИБ привлекаются внешние компании, которые предоставляют консалтинговые услуги в области ИБ, выполняется группой

экспертов, численность которых зависит от целей и задач обследования, а также от сложности объекта оценки. Проведение работ по аудиту ИБ предприятия следует проводить поэтапно. У каждой компании, которая имеет право проводить аудит безопасности, выявляются свои этапы работ. Проведя некоторое исследование, были выявлены основные четыре этапы работ проведения аудита ИБ (рис. 1).

Рисунок 1 – Этапы работ при проведение аудита ИБ.

При планирование работ определяются границы, в рамках которого будет проводиться обследование; порядок и время проведения инструментального обследования ИС заказчика, им является предприятие, в котором проводится аудит ИБ; определяется рабочая группа проекта; п оведения а [1].

При сборе данных необходимо соблюдать точность и полноту информации. От этих факторов будет зависеть качество аудита ИБ. При тщательном изучении различных источников, можно перечислить необходимые данные для аудита ИБ (табл.1) [1].

Таблица 1 – Перечень исходных данных, необходимых для аудита ИБ.

Тип информации	Состав исходных данных
Организационно-распорядительная документация по вопросам информационной безопасности	• политика информационной безопасности ИС; • руководящие документы (приказы, распоряжения, инструкции) по вопросам хранения, порядка доступа и передачи информации; • регламенты работы пользователей с информационными ресурсами ИС.
Информация об аппаратном обеспечении хостов	• перечень серверов, рабочих станций и коммуникационного оборудования, установленного в ИС; • аппаратные конфигурации серверов и рабочих станций; • сведения о периферийном оборудовании
Информация об общесистемном ПО	• сведения об ОС, установленных на рабочих станциях и серверах; • сведения о СУБД, установленных в ИС
Информация о прикладном ПО	• перечень прикладного ПО общего и специального назначения,

	установленного в ИС; • описание функциональных задач, решаемых с помощью прикладного ПО
Информация о средствах защиты, установленных в ИС	• производитель средства защиты; • конфигурационные настройки средства защиты; • схема установки средства защиты
Информация о топологии ИС	• карта локальной вычислительной сети, включая схему распределения серверов и рабочих станций по сегментам сети; • типы каналов связи, используемых в ИС; • используемые в ИС сетевые протоколы; • схема информационных потоков ИС

Анализ и оценка уровня защищенности включают в себя:

- анализ полноты и содержания существующей организационно-распорядительной документации по защите информации [7];
- определение вероятности проведения атаки, а также уровней их ущерба;
- выделение основных информационных активов;
- определение уровня защищенности ИС;
- моделирование действий внешнего и внутреннего нарушителя [7].

На заключительном этапе проведения работ аудита ИБ разрабатываются рекомендации по совершенствованию организационно-технического обеспечения защиты на предприятии. Данные рекомендации в основном содержат типы действий, которые направлены на минимизацию выявленных рисков. Такими действиями являются: уменьшение риска, уклонение то риска, изменение характера риски и в частности понятие риска.

Рисунок 2 – Схема проведения аудита ИБ

Для заключающего момента проведении аудита ИБ необходимо подвести итоги по проведенным этапам работ. Из схемы проведения аудита ИБ (рис. 2) мы

можем увидеть, что результатом аудита является создание документа, который содержит детальную информацию о [4]:

- Всех выявленных уязвимостях объекта аудита;
- Критичности найденных уязвимостях;
- Качественная и количественная оценка рисков ИБ [6];
- Стратегия обеспечения ИБ;
- Последствие в случае реализации угроз;
- Рекомендации по устранению уязвимостей [5].

При достижении цели аудита безопасности предприятия, основываясь на предложенных рекомендациях, имеют возможность произвести оптимизацию структуры информационных технологий (ИТ) и совершенствование процессов ИС. Иными словами возможность построить оптимальную по эффективности и затратам систему защиты информации, соответствующую текущим задачам и целям предприятия. В противном же случае необходимо провести дополнительный анализ данных и с вновь внесенными изменениями создать результирующий отчет по проведенному аудиту [5].

Аудит ИБ – один из наиболее эффективных на сегодняшний день инструментов для получения независимой и объективной оценки текущего уровня защищенности предприятия от угроз ИБ. Благодаря результатам аудита появляется основа формирования стратегии, развития системы обеспечения ИБ предприятий. Но следует заметить, что аудит безопасности должен осуществляться на регулярной основе, это зависит не только от того что любая ИС имеет возможность видоизменятся в ходе работы, но и от увеличения разновидностей угроз безопасности. Только в этом случае аудит ИБ будет приносить пользу и способствовать повышению уровня ИБ предприятий.

Список литературы:

1. Сердюк В.Д. Аудит информационной безопасности (ИБ) [Электронный ресурс]. URL: http://www.bytemag.ru/articles/detail.php?ID=6781 (Дата обращения 02.12.2014 г.)

2. Научно-испытательный институт систем обеспечения комплексной безопасности (НИИ СОКБ). Аудит ИБ [Электронный ресурс]. URL: http://www.niisokb.ru/services/information_security_audit/ (Дата обращения 02.12.2014 г.)

3. ProtectMi – лаборатория безопасности. Аудит и управление ИБ [Электронный ресурс]. URL: http://www.infosecurity.ru/iprotect/audit/ (Дата обращения 02.12.2014 г.)

4. EFSOL – эффективные решения. Аудит ИБ [Электронный ресурс]. URL: http://efsol.ru/promo/info-security-audit.html (Дата обращения 03.12.2014 г.)

5. Pointlane – информационная безопасность. Аудит ИБ [Электронный ресурс]. URL: http://www.pointlane.ru/security_a/ (Дата обращения 03.12.2014 г.)

6. LETA – IT Company. Аудит ИБ [Электронный ресурс]. URL: http://www.leta.ru/services/information-security-management/audit-information-security.html (Дата обращения 04.12.2014 г.)

7. АйТи. Система ИБ. Аудит ИБ [Электронный ресурс]. URL: http://www.it.ru/services/sub/sud_detail.php?ID=383&SUB_ID=6916 (Дата обращения 04.12.2014 г.)