УДК 681.3.06

ПОСТРОЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Ковалева К.А[1]., Глущенко Р.В. [1]

[1]*ФГБОУ ВПО «Ростовский государственный экономический университет»г. Черкесске, Россия (369000, г. Черкесск, ул.Красная, 3), e-mail: kkseniya7979@mail.ru*

Рассмотрены вопросы построения системы информационной безопасности в соответствии со стандартами, предъявляемыми регуляторами по вопросам информационной безопасности в Российской Федерации (ФСБ, ФСТЭК, Роскомнадзор). Для многих компаний, прежде всего, финансовых организаций, производственных холдингов, крупных дистрибьюторов бесперебойная работа ИС, поддерживающих основной бизнес, и доступность данных становятся критичным вопросом.Для проведения качественного аудита информационной безопасности фирме- аудитору должна быть предоставлена исчерпывающая информация об информационной инфраструктуре предприятия и методах ее защиты. Аудит информационной безопасности позволяет объективно и всесторонне оценить текущее состояние системы обеспечения информационной безопасности компании.Необходимым элементом организации работ по обеспечению безопасности информации, ее носителей и процессов обработки в автоматизированной системе организации является определение требуемых степеней защищенности ресурсов.

Ключевые слова:защита информации, аудит информационной безопасности, модели угроз

BUILDING SYSTEMS INFORMATION SECURITY .

Kovaleva K.A.[1], Gluzhenko R.V. [1]

[1]*Branch RGEU " RINH" in Cherkessk , Russia . (369000 , Cherkessk , str. Red , 3), e-mail: kkseniya7979@mail.ru*

The problems of building the information security system in accordance with the standards required by regulators on issues of information security of the Russian Federation (FSB FSTEC , Roscomnadzor) . For many companies , especially financial institutions , industrial holdings, major distributors uninterrupted operation of ICs supporting the core business, and availability of data become critical issue. For quality information security audit firm - auditor should be provided with comprehensive information about the organization's information technology and methods of protection. Information security audit allows an objective and comprehensive evaluation of the current state of information security system company. Essential element of the organization works to ensure the security of information , its carriers and treatment processes in the automated system of the organization is to determine the required degree of security resources.

Keywords: information security, information security audit , the threat model

Введение

В наше время многие российские компании и государственные учреждения решают задачи создания системы информационной безопасности (СИБ), которая соответствовала бы стандартам информационной безопасности (ИБ), предъявляемым регуляторами информационной безопасности в Российской Федерации (ФСБ, ФСТЭК, Роскомнадзор). Такая проблема встает как перед молодыми компаниями (только начинающих свою

деятельность), так и перед предприятиями и организациями, давно присутствующих на рынке, которые приходят к необходимости модернизировать существующую у них информационную инфраструктуру, что зачастую сложнее, чем создать всю систему с нуля.

С одной стороны, необходимость повышения эффективности функционирования СИБ связана с возрастанием количества проблем, связанных с обеспечением ИБ. Здесь необходимо упомянуть растущие требования к обеспечению ИБ со стороны соответствующих регуляторов, так же следует отметить, что российские компании приходят к необходимости учитывать в своей работе, так называемые репутационные риски, а именно ответственность по обеспечению конфиденциальности данных своих клиентов, субподрядчиков, партнеров и т.д. Вместе с тем, в большинстве российских компаний организационная составляющая системы ИБ проработана слабо. Например, данные зачастую не классифицированы, то есть компания не имеет четкого представления о том, какие у нее есть типы данных с позиций их конфиденциальности, критичности для бизнеса, а это влечет за собой целый ряд проблем, начиная от сложностей в обосновании адекватности мероприятий по защите информации и заканчивая невозможностью при возникновении инцидента использовать правовые методы их расследования.

Еще одна немаловажная проблема в сфере защиты информации (ЗИ) связана с обеспечением непрерывности функционирования информационных систем (ИС). Для многих компаний, прежде всего, финансовых организаций, производственных холдингов, крупных дистрибьюторов бесперебойная работа ИС, поддерживающих основной бизнес, и доступность данных становятся критичным вопросом. Сбои в работе систем ведут к прерыванию бизнес-процессов и, соответственно, к недовольству клиентов, штрафам и прочим потерям. А в обеспечении доступности данных немаловажную роль играют системы защиты, предотвращающие злонамеренные атаки на информационную систему (атаки типа «отказ в обслуживании» и др.

С другой стороны, в большинстве Крупных компаний имеет место унаследованная «хаотичная» автоматизация. Развитие корпоративных ИС осуществляется достаточно непродуманно. Чаще всего используется политика «латания дыр», новые ИТ-сервисы добавляются без привязки к уже существующим и без учета их взаимосвязи. И точно так же отсутствует продуманная архитектура системы ИБ, мало кто до настоящего времени определял, насколько система ИБ полная, насколько она покрывает риски, избыточна она или, наоборот, недостаточна и т.д. И что немаловажно - система ИБ редко бывает обоснованной экономически.

Построение СИБ на предприятии можно разделить на четыре части: обследование,

проектирование, внедрение, сопровождение и обслуживание.

Проведение аудита информационной безопасности на предприятии.Прежде чем начинать, строить СИБ на предприятии, необходимо представлять, что уже построено. Для этих целей необходимо провести обследование существующейинформационной инфраструктуры предприятия. На рисунке показана общая структура такого обследования.

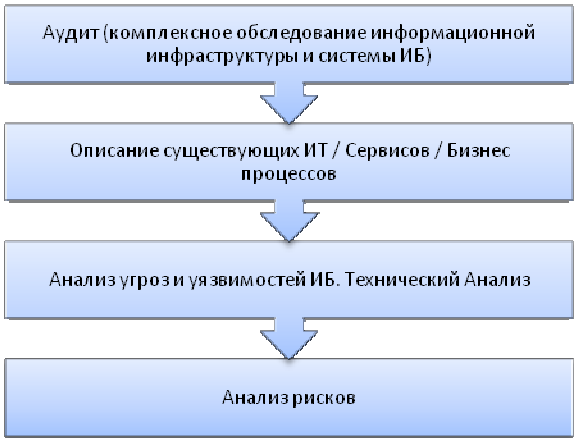

Рисунок 1 – Общая структура обследования.

Для проведения качественного аудита информационной безопасности фирме-аудитору должна быть предоставлена исчерпывающая информация об информационной инфраструктуре предприятия и методах ее защиты. Приведем перечень необходимой информации:

1. Организационно-распорядительная документация по вопросам ИБ: политика информационной безопасности предприятия, руководящие документы по вопросам классификации, обрабатываемой на предприятии информации, ее хранения, порядка доступа к ней и ее передачи, инструкции и регламенты работы администраторов и пользователей с информационными ресурсами АС.

2. Информация об аппаратном обеспечении: перечень серверов, рабочих станций и коммуникационного оборудования, информация о конфигурации используемого оборудования, информация о периферийном оборудовании.

3. Информация о системном программном обеспечении: данные об операционных системах серверов и рабочих станций.

4. Информация о прикладном программном обеспечении: данные о СУБД, прикладных программах и т.д.

5. Информация о средствах информационнойбезопасности:информацияопроизводителе, наличие сертификатов на соответствие средств защиты требованиям регуляторов в области ИБ, данные о конфигурационных настройках СЗИ, схемы установки и методики применения СЗИ.

6. Информация о топологии информационной сети предприятия: топология ЛВС

предприятия, включая разбиение на сегменты, данные о типах каналов связи, топологии, схема информационных потоков в системе, схему подключения к сетям общего пользования.

Как показывает практика, перечисленный выше перечень информации, предоставляется полностью очень редко, поэтому для получения полного объема требуемых данных аудит информационной безопасности на предприятии в большинстве случаев выглядит следующим образом:

1. Фирма заказчик, предоставляет всю имеющуюся у нее информацию и документацию по существующим на фирме информационным системам и методах их защиты. Так же предоставляются все существующие организационно- распорядительные документы по данной тематике.

2. Затем фирма, проводящая аудит раздает опросные листы (анкеты) всем сотрудникам предприятия, которые имеют отношение к функционированию ИС и ее защите. Опросные листы должны быть скорректированы на основе информации, полученной ранее.

3. На третьем этапе представители фирмы-аудитора выезжают на территорию фирмы-заказчика и обследуют ИС, а так же проводят опрос сотрудников, которые работают с ИС, обеспечивают ее работоспособность.

4. На четвертом этапе аудита проводится инструментальный анализ защищенности ИС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы. Данный этап является необязательным, хотя именно он позволяет составить наиболее полную картину защищенности ИС.

5. На пятом этапе сотрудники фирмы-аудитора обрабатывают полученную информацию и пишут отчет о проведенном обследовании.

Аудит информационной безопасности позволяет объективно и всесторонне оценить текущее состояние системы обеспечения информационной безопасности компании. В рамках комплексного аудита может проводиться анализ документации компании в области ИБ, анализ защищенности сетевой инфраструктуры компании, проверка уровня знаний сотрудников в области обеспечения ИБ, анализ процессов и процедур, организационных мероприятий по обеспечению ИБ, разработка моделей возможного нарушителя и угроз.

Также в рамках аудита может быть выполнено тестирование на проникновение и анализ рисков.

Проведение комплексного аудита по информационной безопасности позволяет:

1. получить независимую оценку состояния информационной безопасности в

компании;

2. выявить слабые и потенциально уязвимые места, возможные риски;

3. сформировать детальный план мероприятий по совершенствованию системы обеспечения информационной безопасности, включающий в себя проект бюджета и организационно-штатные мероприятия компании.

По результатам проведенного аудита, в зависимости от условий, заказчику предоставляется пакет документов, который содержит подробный отчет, план мероприятий по совершенствованию/доработке системы ИБ, модели угроз и потенциального нарушителя.

Эффективная реализация, сопровождение и развитие комплекса мер защиты возможны только при наличии формализованного системного подхода к обеспечению информационной безопасности. Для решения этой задачи предназначена система внутренних организационно-распорядительных документов (ОРД) в области информационной безопасности.

Основная цель организационно-распорядительных документов в области информационной безопасности - сформировать интегрированную систему взглядов на цели, задачи, основные принципы и направления деятельности в области обеспечения информационной безопасности с учётом действующего законодательства Российской Федерации, отраслевых и международных стандартов.

В Уставе организации (основном документе, в соответствии с которым организация осуществляет свою деятельность), во всех положениях о структурных подразделениях организации (департаментов, управлений, отделов, служб, групп, секторов и т.п.) и в функциональных обязанностях всех сотрудников, участвующих в процессах автоматизированной обработки информации, должны быть отражены требования по обеспечению информационной безопасности при работе в АС.

Задачи организации и функции по ОИБ ее подразделений и сотрудников в перечисленных выше документах должны формулироваться с учетом положений действующего в России законодательства по информатизации и защите информации (Федеральных Законов, Указов Президента РФ, Постановлений Правительства РФ и других нормативных документов).

Конкретизация задач и функций структурных подразделений, а также детальная регламентация действий сотрудников организации, их ответственность и полномочия по вопросам ОИБ при эксплуатации АС должны осуществляться как путем дополнения существующих документов соответствующими пунктами, так и путем разработки и введения в действие дополнительных внутренних организационно-распорядительных

документов по ОИБ.

В целях обеспечения единого понимания всеми подразделениями и должностными лицами (сотрудниками) организации проблем и задач по обеспечению безопасности информации в организации целесообразно разработать «Концепцию обеспечения информационной безопасности» организации. В Концепции на основе анализа современного состояния информационной инфраструктуры организации и интересов организации в области обеспечения безопасности должны определяться основные задачи по защите информации и процессов ее обработки, намечаться подходы и основные пути решения данных задач.

Необходимым элементом организации работ по обеспечению безопасности информации, ее носителей и процессов обработки вАС организации является категорирование, то есть определение требуемых степеней защищенности (категорий) ресурсов АС (информации, задач, каналов взаимодействия задач, компьютеров). Для обеспечения управления и контроля за соблюдением установленных требований к защите информации и с целью обеспечения дифференцированного подхода к защите конкретных АРМ различных подсистем АС организации необходимо разработать и принять «Положение об определении требований по защите (категорировании) ресурсов» вАС организации. В этом документе необходимо отразить вопросы взаимодействия подразделений организации при определении требуемой степени защищенности ресурсов АС организации в зависимости от степени ценности обрабатываемой информации, характера обработки и обязательств по ОИБ перед сторонними организациями и физическими лицами.

Целесообразно введение классификации защищаемой информации, включаемой в «Перечень информационных ресурсов, подлежащих защите», не только по уровню конфиденциальности (конфиденциально, строго конфиденциально и т.д.), но и по уровню ценности информации (определяемой величиной возможных прямых и косвенных экономических потерь в случае нарушения ее целостности и несвоевременности представления - своевременности решения задач).

В данном Перечне необходимо также указывать подразделения организации, являющиеся владельцами конкретной защищаемой информации и отвечающие за установление требований к режиму ее защиты.

Любые изменения состава и полномочий пользователей подсистем АС должны производиться установленным порядком согласно специальной «Инструкции по внесению изменений в списки пользователей АС и наделению их полномочиями доступа к ресурсам системы».

Меры безопасности при вводе в эксплуатацию новых рабочих станций и серверов, а также при изменениях конфигурации технических и программных средств существующих компьютеров вАС должны определяться "Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств компьютеров АС".

Разработка ПО задач (комплексов задач), проведение испытаний разработанного и приобретенного ПО, передача ПО в эксплуатацию должна осуществляться в соответствии с утвержденным «Порядком разработки, проведения испытаний и передачи задач (комплексов задач) в эксплуатацию».

«Инструкция по организации антивирусной защиты» должна регламентировать организацию защиты АС от разрушающего воздействия компьютерных вирусов и устанавливать ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих АС, за их ненадлежащее выполнение.

«Инструкция по организации парольной защиты» призвана регламентировать процессы генерации, смены и прекращения действия паролей пользователей в автоматизированной системе организации, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

При использовании в некоторых подсистемах АС средств криптографической защиты информации и средств электронной цифровой подписи необходим еще один документ, регламентирующий действия конечных пользователей, - «Порядок работы с носителями ключевой информации».

Для пользователей защищенных АРМ (на которых обрабатывается защищаемая информация или решаются подлежащие защите задачи и на которых установлены соответствующие средства защиты) должны быть разработаны необходимые дополнения к функциональным обязанностям и технологическим инструкциям, закрепляющие требования по обеспечению информационной безопасности при работе в АС и ответственность сотрудников за реализацию мер по обеспечению установленного режима защиты информации.

Регламентация предусматривает введение таких ограничений и внедрение таких приемов работы сотрудников, которые, не создавая помех для исполнения ими своих функциональных обязанностей (технологических функций), минимизируют возможности

Список литературы:

1. Защита персональных данных: 2010 // Искусство управления информационной безопасностью: – Москва.: 2003. / под ред. Слепова Олега.

2. Комплексная защита конфиденциальной информации: Учебно-методическое пособие. – Москва: 11- формат, 2013. – 174. / под ред. А.О. Чефранова, А.Г. Масленникова, Ю.Ф. Алабина.
3. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных".
4. http://ru.wikipedia.org/wiki/Информационная_безопасность
5. http://infoguard.ru/legislation?ID=1&show_id=4&chaper=3