Национальный исследовательский университет

-

Высшая школа экономики

Факультет бизнес - информатики

Кафедра информационной безопасности

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

На тему: «Применение международных стандартов информационной безопасности при деятельности российских коммерческих организаций»

Студент группы № 476

Платонов Андрей Алексеевич

Научный руководитель

Елин Владимир Михайлович

Москва 2013

***Аннотация***

Любая информация нуждается в защите. Существует огромное количество способов ее защиты, к примеру, программных, аппаратных или правовых. С недавнего времени Россия вступила в ВТО и пытается соответствовать международным стандартам, в том числе и международным стандартам информационной безопасности. Для большего соответствия, Россия начала применять класс стандартов ISO 27000 – «Система менеджмента информационной безопасности». Основной целью работы является анализ и сравнительная характеристика международных и российских стандартов, а также сбор рекомендаций и требований системы управления ИБ на основе стандартов ISO 27001 и ISO 27002.

Оглавление

[Введение 3](#_Toc357785465)

[Глава 1.Теоритические основы информационной безопасности 5](#_Toc357785466)

[1.1 Что защищать на предприятии 5](#_Toc357785467)

[1.2 Понятие и задачи информационной безопасности 11](#_Toc357785468)

[1.3 Обзор и сравнение семейства стандартов информационной безопасности ISO 27000 и отечественных стандартов 20](#_Toc357785469)

[Глава 2. Система управления информационной безопасностью 30](#_Toc357785470)

[2.1 Типовая модель нападения 30](#_Toc357785471)

[2.2 Аудит безопасности 34](#_Toc357785472)

[2.3 Информационные риски компании 41](#_Toc357785473)

[2.4 Применение и сбор требований системы менеджмента информационной безопасности, основанных на стандартах ISO 27001 и ISO 27002. 48](#_Toc357785474)

[Заключение 64](#_Toc357785475)

[Список литературы 65](#_Toc357785476)

[Приложение 1 67](#_Toc357785477)

[Приложение 2 68](#_Toc357785478)

[Приложение 3 69](#_Toc357785479)

[Приложение 4 70](#_Toc357785480)

# Введение

В настоящее время большую ценность представляет информация. По этой причине вопросы информационной безопасности играют огромную роль, как в сфере информационных технологий, так и в юридической сфере. Так как факультет бизнес-информатики включает в себя изучение информационной структуры, различных юридических аспектов, а также основам ведения бизнеса, темой моей работы будет являться анализ и разработка собственных требований (на основе международных стандартов), которые необходимы для качественного внедрения системы менеджмента информационной безопасности на российском предприятии. Данная тема довольно актуальна, так как защита информации на предприятии, позволяет преобразовать компанию в конкурентоспособную, что позволит ей получать больше прибыли и стать неуязвимой для злоумышленников.

Проблемой внедрения качественной системы управления безопасностью на российское предприятие, является тот факт, что в России отсутствуют четкие стандарты, которым можно следовать для обеспечения безопасности.

В своей работе я рассматриваю различные аспекты данной проблемы и предлагаю решения путем предоставления требований, основанных на различных международных стандартах.

Целью исследования данной работы является выделение всех недостатков стандартов, которые относятся к информационной безопасности за весь промежуток времени существования стандартов, а также анализ требований и предоставление рекомендаций, на основе стандартов, по внедрению системы менеджмента информационной безопасности.

Для достижения заявленной цели, необходимо решить следующие задачи:

1. Выделение объектов, для защиты на предприятии;
2. Проведение сравнительной характеристики международных и отечественных стандартов;
3. Анализ и разработка типовой модели нападения на предприятие;
4. Анализ системы управления информационной безопасностью
5. Рассмотрения аудита компании;
6. Рассмотрение информационных рисков компании;

Объектом исследования является система управления информационной безопасностью в Российских коммерческих структурах.

В своей работе я рассматриваю различные аспекты данной проблемы и предлагаю решения путем предоставления требований, основанных на различных международных стандартах.

# Глава 1.Теоритические основы информационной безопасности

# Что защищать на предприятии

Система федерального законодательства включает себя огромное количество актов, относительно различных видов тайн. В данной работе приведены основные тайны, которые необходимо защищать от несанкционированного доступа. Всю информацию на предприятии можно разделить на несколько типов тайн, которые должны быть подвергнуты защите. Однако основной информацией, которая нуждается в защите, является конфиденциальная информация. К конфиденциальной информации указом президента № 188 «Об утверждении Перечня сведений конфиденциального характера» относится:

* «Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
* Сведения, составляющие тайну следствия и судопроизводства.
* Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом и федеральными законами (служебная тайна).
* Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией и федеральными законами (врачебная, нотариальная, адвокатская тайны, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
* Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом и федеральными законами (коммерческая тайна).
* Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них».[[1]](#footnote-1)

 «Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду».[[2]](#footnote-2) Стоит отметить, что защите подлежит любая информация, которая находится в документированном виде на предприятии. Неправомерное обращение стороннего лица с одной из тайн компании может привести к серьезному ущербу предприятия. На основе ГК РФ (ст. 139) к коммерческой тайне можно отнести следующие документы:

* Документы о платежеспособности;
* Учредительные документы;
* Различные сведения об установленных формах отчетности о правильности уплаты налогов;
* Сведения о численности, составе работающих, заработной плате и условиях труда;
* Сведения об уплате налогов;
* Сведения о лицах, которые работают на предприятии и занимаются предпринимательством.

Собственник данной информации имеет полное право в отказе подачи данной информации на законном основании. Стоит также отметить, что при нарушении прав пользователя коммерческой информации применяются следующие санкции, на основе статьи 183 УК – «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»:

* «Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев либо лишением свободы на срок до двух лет.
* Незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб, наказываются штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев либо лишением свободы на срок до трех лет со штрафом в размере до пятидесяти минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного месяца либо без такового».[[3]](#footnote-3)

Патентная тайна является следующим типом конфиденциальной информации. Чумарин вводит следующее определение патентной тайны: «тайна сведений о сущности изобретения, полезной модели или официальной публикации о них».[[4]](#footnote-4) Защите данной тайны уделяется огромное количество времени организациями, которые ведут научные разработки. Патентная тайна – это различного рода сведения, которые могут содержаться для изобретений. На основе патентного закона Российской федерации патентная тайна может содержать следующее:

* Формула какой-либо модели;
* Реферат;
* Чертежи, рисунки, фотографии, на которых изображено изобретаемое изделие.

Также патентная тайна может содержать в себе личные данные об изобретателе. Неразглашение о патентной тайне действует шесть месяцев. При нарушении правил о неразглашении патентной тайны грозят следующие наказания (на основе статьи 147 УК – «Нарушение изобретательских и патентных прав»):

1. «Незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб, -

 наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

 2. Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой,  наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо принудительными работами на срок до пяти лет, либо арестом на срок до шести месяцев, либо лишением свободы на срок до пяти лет».[[5]](#footnote-5)

Каждый сотрудник, работающий на предприятии, обладает персональными данными. При подаче заполнении трудового договора и анкеты, работник предоставляет больше персональной информации, чем действующие минимальные данные о гражданине, тем самым подписывая договор, он возлагает ответственностью организацию, на которую он работает. Минимальные данные, которые гражданин обязан предоставить при просьбе уполномоченного лица, являются следующими:

* Фамилия;
* Имя;
* Отчество;
* Пол;
* Дата рождения.

Любая организация обладает счетом в банке. Банковская тайна – это «тайна об операциях, о счетах и вкладах своих клиентов и корреспондентов».[[6]](#footnote-6) При заключении договора с банком (открытие счета), банк подписывает условия неразглашения следующей информации (статья 857 УК – «Банковская тайна»):

* «Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте;
* Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законом;
* В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков».[[7]](#footnote-7)

Стоит отметить тот факт, что обладателем банковской тайны является не только организации, то и все физические и юридические лица, которые имеют счета в банке.

При судебном процессе любой человек, а также организация облагается адвокатской тайной. Данная тайна относится к профессиональному типу. При судопроизводстве сведения, которые составляют адвокатскую тайну, являются:

* Сведения, которые были сообщены юристу, при оказании компании юридической помощи;
* Любые обстоятельства, которые стали известны адвокату, как защитника.

Стоит отметить тот факт, что если в рамках суда используется коммерческая тайна предприятия, то адвокат обязан все равно сохранять коммерческую тайну и не использовать в качестве аргументов защиты.

##  Понятие и задачи информационной безопасности

Перед описанием стандартов информационной безопасности следует сначала определить: что же такое информационная безопасность. Данное понятие можно рассматривать с нескольких сторон: как состояние и как деятельность.

* Состояние (качество) определённого объекта. В качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства и т. п.;
* Деятельность, направленная на обеспечение защищённого состояния объекта (в этом значении чаще используется термин «защита информации»)

В данной работе информационная безопасность будет рассматриваться как деятельность. Принято считать, что информационная безопасность - это комплекс мероприятий, обеспечивающий следующие факторы:

* Конфиденциальность
* Целостность
* Доступность

Целостность подразумевает под собой возможность передачи информации и работы с ней без ее потери или видоизменения. Возможностью изменения информации должны обладать уполномоченные лица. «Конфиденциальность (от англ. confidence — доверие) — необходимость предотвращения утечки (разглашения) какой-либо информации».[[8]](#footnote-8)Чаще всего такой информацией может, является служебная тайна или «ноу-хау». Пользователю необходим доступ к своей информации в любой промежуток времени. Осуществляться он может с помощью авторизации лица. Фактор, отвечающий за этот процесс, называется доступностью. «Целостность информации (также целостность данных) — термин в информатике и теории телекоммуникаций, который означает, что данные полны, условие того, что данные не были изменены при выполнении любой операции над ними, будь то передача, хранение или представление». [[9]](#footnote-9)В данной работе были перечислены основные факторы, которые используются в любой литературе при описании информационной безопасности. Основной целью данного понятия является соблюдение и обеспечение всех факторов информационной безопасности. Для выполнения всего вышеперечисленного применяются механизмы.

«идентификация — определение (распознавание) каждого участника процесса информационного взаимодействия[[10]](#footnote-10)», перед тем как к нему будут применены понятия информационной безопасности;

«аутентификация — обеспечение уверенности в том, что участник процесса обмена информацией идентифицирован верно;

контроль доступа — создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа».[[11]](#footnote-11)

«Авторизация (от англ. authorization — разрешение, уполномочивание) — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий;[[12]](#footnote-12)

«аудит и мониторинг — отслеживание событий, происходящих в процессе обмена информацией (аудит предполагает анализ событий постфактум, а мониторинг реализуется в режиме реального времени;

реагирование на инциденты — совокупность процедур или мероприятий, выполняемых при нарушении или подозрении на нарушение информационной безопасности;

управление конфигурацией — создание и поддержание функционирования среды информационного обмена в работоспособном состоянии и в соответствии с требованиями информационной безопасности;

управление пользователями — обеспечение условий работы пользователей в среде информационного обмена в соответствии с требованиями информационной безопасности.

управление рисками — обеспечение соответствия возможных потерь от нарушения информационной безопасности мощности защитных средств (то есть затратам на их построение);

обеспечение устойчивости — поддержание среды информационного обмена в минимально допустимом работоспособном состоянии и соответствии требованиям информационной безопасности в условиях деструктивных внешних или внутренних воздействий».[[13]](#footnote-13)

За счет данных механизмов происходит достижение целей информационной безопасности. Стоит отметить, что аутентификация сама по себе не может быть целью информационной безопасности. Данный механизм можно выделить как метод определения участника информационного обмена, который определяет политику в отношении конфиденциальности или доступности, которая должна быть применена к данному участнику.

Рассмотрим с помощью, каких инструментов происходит реализация перечисленных выше механизмов. Описание всех инструментов невозможно, так как их использование зависит от ситуации. Объём и количество применяемых инструментов может колоссально варьироваться. Часто бывает так, что некоторые механизмы переходят в средства и наоборот. Приведем пример. Персонал производит аудит, который обеспечивает учет. Из этого следует, что персонал – это средство, аудит – механизм, а учет – это цель. Другим примером может послужить хранение паролей в зашифрованном виде. Здесь ситуация обстоит иначе. Криптография является средством защиты паролей, пароли используются для механизма, который называется аутентификация, а аутентификация обеспечивает один из факторов информационной безопасности – целостность.

Перечислим основные инструменты:

* Персонал;
* Нормативное обеспечение;
* Модели безопасности;
* Криптография;
* Антивирусное обеспечение;
* Межсетевые экраны;
* Сканеры безопасности;
* Системы обнаружения атак;
* Резервное копирование;
* Резервирование;
* Аварийный план;
* Обучение пользователей.

Как мы можем видеть, информационная безопасность в качестве инструментов может использовать как человеческие ресурсы, так и программное обеспечение, и различные документы. Под персоналом подразумеваются люди, которые будут вести процесс внедрения информационной безопасности на предприятие. Более того, они также будут заниматься всем обеспечения информационной безопасности, а именно: разработка, внедрение, поддержка, контроль, доработка.

Нормативное обеспечение включает в себя различные документы, помогающие персоналу внедрять систему информационной безопасности. Эти документы могут состоять из следующих инструкций:

* Межгосударственные стандарты;
* Государственные стандарты России;
* Своды правил;
* Руководящие документы системы;
* Общероссийские нормы технологического проектирования;
* Отраслевые стандарты;
* Инструкции, методические указания, пособия;
* Рекомендации по проектированию

Документы могут меняться в зависимости от направления деятельности предприятия. Бумаги, предоставленные в данной работе, соответствуют типичной строительной компании. Модели безопасности – это различные схемы, которые заложены в определенной информационной системе. Криптография – это очень сложный алгоритм защиты информации. Другими словами – это методы и средства преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею (чтение и/или модификацию), вместе с методами и средствами создания, хранения и распространения ключей - специальных информационных объектов, реализующих эти санкции.

Под антивирусным обеспечением понимается программное средство, которое обеспечивает защиту различного рода информации от проникновения в нее нежелательного программного обеспечения, с целью редактирования или похищения информации. В ходе работы был проведен анализ самого лучшего антивируса в мире. Рейтинг антивирусного программного обеспечения был предоставлен независимой тестовой компанией Virus Bulletin. Испытания проводились на платформе Windows XP Professional SP3. TrustPort определил 95,24% вредоносных образцов и подтвердил лидирующую позицию среди самых мощных антивирусов в мире.

В приложении 1 изображена итоговая таблица, в которой можно наблюдать какое место в мире занимают антивирусы TrustPort (положение антивирусов в таблице определено результатами последних четырех тестирований).

Межсетевые экраны – это устройства, которые контролируют доступ из одной информационной сети в другую. «Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации» , - повествует сайт википедии. Среди возможностей данного инструмента информационной безопасности, стоит выделить следующее:

* фильтрация доступа к заведомо незащищенным службам;
* препятствование получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;
* контроль доступа к узлам сети;
* может регистрировать все попытки доступа как извне, так и из внутренней сети, что позволяет вести учёт использования доступа в Интернет отдельными узлами сети;
* регламентирование порядка доступа к сети;
* уведомление о подозрительной деятельности, попытках зондирования или атаки на узлы сети или сам экран;

Сканеры безопасности (уязвимостей) – это программные или аппаратные средства, которые служат для мониторинга сетевых компьютеров. В приложении 1, можно видеть для каких целей может использоваться сканер безопасности.

 Системы обнаружения атак - устройства мониторинга активности в информационной среде, иногда с возможностью принятия самостоятельного участия в указанной активной деятельности.

Резервное копирование и дублирование – это виды инструментов, предназначенные для обеспечения безопасности при утере или возможности утери информации. Резервное копирование подразумевает под собой сохранение избыточного количества информационных ресурсов при возможности утраты. Дублирование - это создание альтернативных устройств, которые необходимы для функционирования информационной среды, в случае выхода из строя одной или более средств поддержки.

Аварийный план - набор мероприятий, предназначенных для претворения в жизнь, в случае если события происходят или произошли не так, как было предопределено правилами информационной безопасности. Обучение пользователей - подготовка активных участников информационной среды для работы в условиях соответствия требованиям информационной безопасности.

Возможно, что часть понятий укрупнено, часть из них детализировано. Основной целью предоставления данного списка было показать типовой выбор инструментария для предприятия, развивающего информационную безопасность.

Рассмотрим основные направления информационной безопасности. Среди них стоит выделить:

* Физическая безопасность;
* Компьютерная безопасность.

Физическая безопасность — обеспечение сохранности самого оборудования, предназначенного для функционирования информационной среды, контроль доступа людей к этому оборудованию.[[14]](#footnote-14) Дополнительно сюда может быть включено понятие защиты самих пользователей информационной среды от физического воздействия злоумышленников, а также защиты информации не виртуального характера (твердых копий — распечаток, служебных телефонных справочников, домашних адресов сотрудников, испорченных внешних носителей и т. п.)

Компьютерная безопасность (сетевая безопасность, телекоммуникационная безопасность, безопасность данных) — обеспечение защиты информации в ее виртуальном виде.[[15]](#footnote-15) Стоит выделить этапы нахождения информации в среде, и по этим принципам разделять, например, компьютерную (на месте создания, сохранения или обработки информации) и сетевую (при пересылке) безопасность, но это, в принципе, нарушает комплексную картину безопасности.

 Единственное, с чем логично было бы согласиться, — это термин безопасность данных, или скорее, безопасность данных в рамках данного приложения. Дело в том, что в конкретном программном комплексе модель безопасности может быть реализована таким образом, что это потребует отдельного специалиста (или даже службы) по ее поддержанию. В этом случае, возможно, разделить понятия безопасность данных (конкретного приложения) и безопасность сети (всей остальной информационной среды).

Далее хотелось бы выделить ряд глобальных задач информационной безопасности.

* Формализация и реализация единой государственной политики по обеспечению защиты национальных интересов от угроз в информационной сфере;
* Совершенствование законодательства различных стран в сфере обеспечения информационной безопасности;
* Определение и назначение должностных органов государственной власти, субъектов и органов местного самоуправления в сфере обеспечения информационной безопасности;
* Координация деятельности органов государственной власти по обеспечению информационной безопасности;
* Создание условий для успешного развития информационной безопасности, осуществления эффективного гражданского контроля над деятельностью органов государственной власти;
* Совершенствование и защита информационной инфраструктуры, ускорение развития новых информационных технологий и их широкое распространение;
* Развитие стандартизации информационных систем на базе общепризнанных международных стандартов и их внедрение для всех видов информационных систем;
* Создание оптимальных социально-экономических условий для осуществления важнейших видов творческой деятельности и функционирования учреждений культуры;
* Противодействие угрозе развязывания противоборства в информационной сфере;
* Организация международного сотрудничества по обеспечению информационной безопасности при интеграции различных стран в мировое информационное пространство.

# 1.3 Обзор и сравнение семейства стандартов информационной безопасности ISO 27000 и отечественных стандартов

 «ISO/IEC 27000 — серия международных стандартов, включающая стандарты, по информационной безопасности, опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC). Серия содержит лучшие практики и рекомендации в области информационной безопасности для создания, развития и поддержания Системы Менеджмента Информационной Безопасности» - сообщает нам сайт Википедии. Данное семейство включает в себя Международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.

Для этого семейства стандартов используется последовательная схема нумерации, начиная с 27000 и далее. На данный момент опубликовано 17 стандартов данного семейства. Приступим к описанию.

 По стандарту ISO 27001:2005 информационная безопасность – это: “обеспечение конфиденциальности, целостности и доступности информации; также возможно обеспечение и других свойств, таких как аутентичность, идентифицируемость, отказоустойчивость и надёжность[[16]](#footnote-16)”

Стоит разделить все стандарты на 4 группы:

* Стандарты для обзора и введения в терминологию;
* Стандарты, определяющие обязательные требования к СУИБ (система управления информационной безопасностью);
* Стандарты, определяющие требования и рекомендации для аудита СУИБ;
* Стандарты, предлагающие лучшие практики внедрения, развития и совершенствования СУИБ.

Давайте рассмотрим каждый стандарт из данного семейства.

**Стандарты для обзора и введения в терминологию.** К данной группе можно отнести первый стандарт семейства: ISO 27000. ISO 27000 включает в себя: информационные технологии, средства обеспечения безопасности, системы менеджмента информационной безопасности а также обзор и словарь. Другими словами, стандарт описывает основные определения, которые используются в стандартах информационной безопасности.

 **Стандарты, определяющие обязательные требования к СУИБ.** Данная группа включает в себя всего лишь один стандарт: ISO 27001. Суть этого стандарта заключается в описании информационных технологий, методов и средств обеспечения безопасности, менеджмента информационной безопасности и выявлении требований. Стоит сказать, что это основной стандарт группы. ISO 27001 определяет требования к разработке, внедрению и улучшению менеджмента информационной безопасности.

**Стандарты, определяющие требования и рекомендации для аудита СУИБ.** В отличие от предшествующих групп, в данную - можно включить три стандарта: ISO 27006, ISO 27007, ISO 27008. Не сложно догадаться, что данные стандарты включают в себя указания и требования для аудита информационной безопасности. Однако давайте рассмотрим каждый стандарт отдельно. ISO 27006 включает в себя: описание информационных технологий, средств обеспечения информационной безопасности и требования для организаций, которые выполняют аудит систем менеджмента информационной безопасности. ISO 27007 описывает два первых пункта ISO 27006, а также указания для аудита систем менеджмента информационной безопасности. Данный стандарт очень полезен для аудиторов организаций. ISO 27008 включает в себя руководство для аудитор по мерам обеспечения ИБ. Данный стандарт специализирован на аудите информационной безопасности в организации.

**Стандарты, предлагающие лучшие практики внедрения, развития и совершенствования СУИБ.** Эта группа включает в себя оставшиеся стандарты семейства 27000, а именно стандарты:

* ISO 27002;
* ISO 27003;
* ISO 27004
* ISO 27005
* ISO 27011
* ISO 27031
* ISO 27033
* ISO 27034
* ISO 27035
* ISO 27799 ( специализированной руководство СУИБ в здравоохранении)
* ISO 24762

Приступим к описанию данных стандартов. ISO 27002 включает в себя описание средств обеспечения информационной безопасности, а так же свод практики менеджмента информационной безопасности. Данный стандарт предоставляет указания для внедрения, разработки, поддержки и совершенства СУИБ. Можно назвать это основным стандартом для консультантов. В отличие от ISO 27002, ISO 27003 предоставляет руководство по осуществлению контроля информационной безопасности. Стандарт дает указания и методику для процессов разработки и внедрения СУИБ. Измерения менеджмента ИБ предоставлено в ISO 27004. Данный стандарт рассчитан для проектирования, выбора, улучшения методов измерения эффективности системы. ISO 27005 помогает рассмотреть различные методы защиты, а также управления рисками при ИБ. Можно назвать данный стандарт самым важным в группе, так как рассмотрение рисков является основой при обеспечении информационной безопасности.ISO 27011 специализируется на телекоммуникациях. Основа стандарта заключается в описании обеспечения информационной безопасности по СУИБ в телекоммуникационных организациях. Любая компания проводит глубокий анализ по обеспечению непрерывности своего бизнеса. Стандарт ISO 27031 поможет в этом. В нем можно найти руководство по менеджменту ИБ для телекоммуникаций.

Информационную безопасность можно разделить на несколько типов. Сетевая безопасность является одним из типов ИБ. Методы защиты информации и обеспечение сетевой безопасности подробно описаны в стандарте ISO 27033. Также здесь можно найти информацию о различных угрозах, методах проектирования сетевой инфраструктуры.

ISO 27034 несет терминологический характер. Здесь можно узнать информацию о безопасности приложений, а также методах обеспечения безопасности данного программного обеспечения. Об управлении инцидентами по ИБ можно узнать из ISO 27035. Данный стандарт является одним из ценных стандартов в группе развития и совершенствования СУИБ.

Последние два стандарта являются специализированными. ISO 27799 специализируется на здравоохранении. Он описывает информатику в здравоохранении. ISO 24762 относится к информационным и коммуникационным технологиям. В нем описаны методы защиты, а также рекомендации по услугам для аварийного восстановления ИКТ. В данной главе были описаны все возможные стандарты данного семейства. Группа стандартов ISO 27000 получила очень серьезное развитие в последние годы.

**Обзор отечественных стандартов**

Исторически сложилось, что в России проблемы информационной безопасности изучались и своевременно решались, специализировавшись на охране государственной тайны. Проанализировав принятые стандарты в России, можно сказать, что она очень отстает от Европы. На сегодняшний день насчитывается порядка 30 отечественных стандартов.

Проблема защиты информации на предприятиях имеет свои особенности, которые необходимо учитывать, поскольку они оказывают серьезное влияние на информационную безопасность (ИБ).

**Приоритет экономических факторов**. Необходимо максимально снизить финансовые потери и предоставить пользователям возможность получать прибыль. Важным условием при этом, в частности, является минимизация типично банковских рисков (например, потерь за счет ошибочных направлений платежей, фальсификации платежных документов и т. п.). Необходимо обеспечить открытость проектирования, которая будет предусматривать разработку системы защиты информации.

**Юридическая значимость коммерческой информации**[[17]](#footnote-17), которую можно определить как свойство безопасной информации, позволяющее обеспечить юридическую силу электронным документам или информационным процессам в соответствии с законодательством Российской Федерации.

В 1999 году, был введен международный стандарт ISO 15408, который в области обеспечения ИБ имел большое значение, как для разработчиков компьютерных ИС, так и для их пользователей. Стандарт ISO 15408—2002 стал своего рода гарантией качества и надежности сертифицированных по нему программных продуктов.

ГОСТ Р ИСО/МЭК 15408-2002 состоит из трех частей. Часть 1 (ГОСТ Р ИСО/МЭК 15408-1 «Введение и общая модель») устанавливает общий подход к формированию требований безопасности и оценке безопасности.

На их основе происходит разработка основных конструкций, которые представляют требования безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ.

Часть 2 (ГОСТ ИСО/МЭК 15408-2 «Функциональные требования безопасности») содержит различные функциональные требования безопасности и предоставляет возможность их детализации и расширения.

Часть 3 (ГОСТ ИСО/МЭК 15408-3 «Требования доверия к безопасности») включает систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям.

ГОСТ 50739 описывает способы защиты от несанкционированного доступа. Данный стандарт устанавливает единые функциональные требования к защите средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к информации; к составу документации на эти средства, а также номенклатуру показателей защищенности СВТ, описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации.[[18]](#footnote-18)

ГОСТ Р 50922-96 несет методологический характер. Он включает в себя основные термины и определения по информационной безопасности.

Защита от вирусов является первостепенной задачей при защите информационно безопасности. ГОСТ Р 51188-98 содержит в себе типовое руководство по по испытанию ПО на наличие вирусных программ.  «Настоящий стандарт распространяется на испытания программных средств (ПС) и их компонентов, цели которых - обнаружить в этих ПС и устранить из них компьютерные вирусы (KB) силами специальных предприятий (подразделений), и устанавливает общие требования к организации и проведению таких испытаний» [[19]](#footnote-19)- ГОСТ 51188-98.

ГОСТ 51275-99 описывает общие положения о защите информационной безопасности и некоторые факторы, которые на нее воздействуют.

ГОСТ 7498-1 и ГОСТ 7498 – 2 описывают базовую эталонную модель информационной технологии по защите информационной безопасности. Можно сказать, что эти стандарты являются библией специалистов ИБ. В одном этих стандартов указано описание данной эталонной модели, в то время как в другой, описана архитектура защита информации в открытых системах.

Последующие три стандарта специализируются на криптографической защите. Первый из них включает в себя описание алгоритма криптографического образования. По некоторым сведениям, история этого шифра гораздо более давняя. Алгоритм, положенный впоследствии в основу стандарта, родился, предположительно, в недрах Восьмого Главного управления КГБ СССР. ГОСТ 34 10 описывает различные методы по проверке подлинности электронной подписи. Данный стандарт также включает в себя алгоритм, однако, не для защиты информации, а для формирования проверки цифровой подписи. Последний стандарт несет программистский характер. ГОСТ 3411 -91 описывает функцию хэширования. «Хеширование (иногда «хэширование», англ. hashing) — преобразование по детерминированному алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины», - сообщает сайт Википедии.

**Сравнительный анализ зарубежных и отечественных стандартов**

На сегодняшний день количество европейских стандартов в разы превышает отечественные. Примером может случить тот факт, что вступило в силу порядка 30 отечественных стандартов. Проведя обзор ISO 27000 являющимся семейством стандартов, которые насчитывает порядка 19 стандартов, можно сделать вывод о заочном проигрыше отечественных стандартов. Однако если мы проведем сравнительный анализ, то увидим, что основы, которые способствуют минимальной защите ИБ, присутствуют в России.

Критерием нашего сравнения будет служить четыре группы, которые мы выделили, при описании ISO 27000.

**Терминология.** К данной группе относится по одному стандарту из каждого стандарта – отечественного и зарубежного. В каждом из стандартов даны четкие определения информационной безопасности. Одна есть и отличия. Отечественный стандарт больше специализируется на терминологии защиты информации и угроз ее потери. В данном стандарте преобладают такие определения как защита информации от утечки, защита информации от разглашения, система защиты информации, цель защиты информации. Европейский стандарт больше специализируется на правах доступа к информации отдельных лиц. В ISO 27000 можно увидеть информацию о таких определениях как аутентификация, доступность, конфиденциальность, событие, результативность. Вполне возможно, что такое отличие в практически одинаковых названиях стандартов связано с отличием менталитета в Европе от России.

**Определение требований к СУИБ.** В данную группу опять же входят по одному стандарту из зарубежного и отечественного стандарта. Стандарт ISO 27001 от зарубежных стран и ГОСТ 15408 в трех главах от России. Европейский стандарт описывает четко и ясно алгоритм внедрения системы моделирования информационной безопасности. Ниже я предоставлю 4 первых пункта.

1. Первый этап.
* Осознать цели и выгоды внедрения СМИБ
* Получить поддержку руководства на внедрение и ввод в эксплуатацию СМИБ
* Распределить ответственность по СМИБ
1. Второй этап. Организационный
* Создать группу по внедрению и поддержке СМИБ
* Обучить группу по внедрению и поддержке СМИБ
* Определить область действия СМИБ
1. Третий этап. Первоначальный анализ СМИБ
* Провести анализ существующей СМИБ
* Определить перечень работ по доработке существующей СМИБ
1. Четвертый этап. Определение политики и целей СМИБ
* Определить политику СМИБ
* Определить цели СМИБ по каждому процессу СМИБ

Отечественные стандарт разделен на 3 главы для описания полноты процесса. В первой главе происходит описание некоторых определений и предоставляется алгоритм обеспечения ИБ. Во второй главе происходит описание функциональных требований к информационной безопасности, которые также представлены в виде списка. Третья также как и вторая содержит правила в виде списка, однако, предоставляя требования для доверия к безопасности. Зарубежные стандарты рассматривают все это в отдельных стандартах, не смешивая это так, как делает Россия.

**Требования и рекомендации аудита СУИБ.** ГОСТ 51 -275 99 а также ГОСТ 7498 -1 можно отнести к данной группе. Базовая эталонная система обеспечения безопасности открытых систем – вот, что предоставила Россия Европе. Подробное рассмотрение модели и описание того, как должна быть структурирована открытая система для проведения аудита и обеспечения качественной защиты ИБ – вот, что включает в себя данный стандарт. Так же как и предыдущих стандарт, она разделен на две главы, однако, здесь, это упрощает понимание. Анализ факторов, которые могут быть использованы для защиты информации, вместе с эталонной моделью предоставляют хотя и неполные, однако достаточные сведения для аудита СУИБ.

Европейские стандарты отличаются краткостью и лаконичностью своих изъяснений. Их стандарт даже называется как «требования для аудита информационной безопасности».

**Предложение лучшей практики внедрения, развития и совершенствования СУИБ.**

Здесь, априори, первенство занимают европейские стандарты. Стоит отметить, что они выигрывают количеством в данной группе. Чёткое и ясное название стандартов, например, «свод практики менеджмента информационной безопасности», предоставляет проектирование, выбор, улучшение методов измерения эффективности системы. Более того, присутствие специализированных стандартов в области здравоохранения, являются огромным плюсом в европейских стандартах. Это доказывает тот факт, что заграницей информационная безопасность распространена везде на все слои информации индивидуума. Другими словами, защита происходит не только от краж, то и от разглашения фамилии или заболеваний, если того хочет человек. Специализация российских стандартов направлена на сохранения материального статуса компаний и человека. Защита банковских карт, счетов в банке, номера кредитных карт: все это защищено. К этой группе можно отнести стандарты, относящиеся к криптографической защите, а также к стандартам, специализирующимся на испытания ПО на наличие вирусов.

#

# Глава 2. Система управления информационной безопасностью

# Типовая модель нападения

В данной главе будет рассмотрен процесс хакерской атаки. Перед тем, как приступить к описанию данного процесса стоит выделить некую классификацию атак. Данную классификацию можно разделить на три типа:

* Локальная атака;
* Удаленная атака;
* Атака на поток данных.

Под локальной атакой можно понимать некую физическую атаку, то есть, когда злоумышленник оказался рядом с компьютером жертвы.

Удаленная атака – это тип атаки, когда злоумышленник не видит ту рабочую станцию, с которой он производит хакерскую атаку. Более того компьютер жертвы в этот момент не проявляет никакой активности.

Атака на поток данных – это случай, при котором компьютер жертвы участвует в атаке на определенных сетевой сегмент, передовая информацию между собой.

Первое, о чем должен задуматься хакер — об отсутствии обратной связи. Другими словами, злоумышленник должен обеспечить себе условия, при которых жертва (или тот, кто будет действовать в его интересах) не сможет опознать или идентифицировать хакера, который произвел атаку на компьютер. Не умелые хакеры используют динамических IP –адрес, однако существуют утилиты, которые способны отследить как минимум провайдер злоумышленника. Проанализировав регистрационный журнал, можно незамедлительно найти хакера.

Необходимы другие методы. Стоит выделить несколько таковых:

* Физический;
* Логический.

 Физический метод подразумевает под собой постоянное изменение физического места атаки. Однако, этот метод приемлем только для краткосрочной работы (несколько дней, а иногда и часов). Используя данный метод, хакер, рискует быть быстро определённым по городу или стране, а далее за поиск возьмутся соответствующие службы. Более того, переезд из одного города в другой довольно дорогостоящий.

Логический метод – наиболее распространен среди злоумышленников. Он подразумевает отсутствие переездов, а использование серверов в интернете, которые предоставляют свои адреса для анонимной работы в Интернете. При работе с таким сервисом, достаточно знать адрес атакуемого компьютера. Хакер указывает специальным образом адрес жертвы вместе с адресом прокси-сервера.

Анонимайзер скроет настоящий адрес хакера, заменив его в случае поиска его специальными службами. Это приведет к тому, что в атакуемой системе можно будет увидеть только адрес прокси-службы, который в большинстве находится далеко от злоумышленника. Прописывая атакующий запрос, используя несколько аномайзеров, хакерам довольно легко спрятать свой реальный адрес. Однако использование анонимайзеров поддерживается не всеми сетевыми протоколами.

Специалист по безопасности все – таки может узнать адрес прокси – службы, так как хакер узнал его. Если вносить такие сервера в «черный» список межсетевого экрана, это может привести к блокированию атаки с данного адреса.

Стоит отметить что, правоохранительные органы и государственные службы имеют возможность отследить использование анонимайзеров и других удаленных сервисов кардинально другим способом. Все зависит от опасности, причиненной хакером.

Несмотря на многообразие самостоятельных провайдеров, топология сети Интернет представляет собой паутину только относительно нескольких центральных узлов. Все периферийное виртуальное пространство представлено в виде структуры, которая расползается от центра. Необходимо поставить оборудование мониторинга в нескольких узлах и организациям будет предоставлен полный доступ к объему трафика сети.

Объем такого трафика принимает огромные значения, что довольно сильно затрудняет процесс фильтрования трафика.

Однако поддержка журналов, состоящих только из IP-адресов/номеров портов источника и получателя трафика, времени установки и завершения сессии, вполне реальна. NetFlow является одним из сетевых стандартов для таких журналов. Проектирование было разработано таким образом, что их возникновение отнимает малую часть вычислительных ресурсов маршрутизатора. Приведем пример.

Пусть известно, что компания A была взломана с адреса B с использованием средства C. Предположим, что есть доступ к электронным журналам, чтобы узнать:

* кто за последние дни (недели) интересовался сайтом;
* кто скачивал (или использовал) средство С;
* кто использовал прокси-сервис А.

Сравнив результаты, можно существенно снизить область поиска.

Допустим хакер не готов для атаки. Что еще ему нужно для начала? Адрес веб-сервера или шлюза организации? Быть может, пойти немного другим путем?

В таком случае необходимо узнать несколько телефонов организации. Получив данную информацию можно узнать не подключен ли кто-нибудь из них к модему. War – Dialer: программа, которая будет обзванивать номера до тех пор, пока не отметит все телефоны, которые подключены к модему.

Стоит отметить, что, именно модемам служба обеспечения безопасности уделяет недостаточно внимания, оставляя их включенными во внерабочее время, что в дальнейшем приводит к взлому информационной системы предприятия.

Перед тем как произвести атаку необходимо узнать топологию атакуемой сети. Программы трассировки сетевых маршрутов и генерации фальшивых пакетов помогут хакеру выяснить расположение маршрутизаторов, межсетевых экранов. Более того данные программы предоставляют возможность проходить через межсетевые экраны при их неправильной конфигурации.

Следующим шагом исследований злоумышленника, скорее всего, станет сканирование портов. Обычно оно применимо к сетям, работающим на основе TCP/IP. Для сканирования портов существует специальное программное обеспечение, которое работает без участия человека (например, ночью) и может быть легко загружено с известных хакерских сайтов.

# 2.2 Аудит безопасности

Так как практической частью данного диплома является практическое применение стандарта ISO 27001, который описывает рекомендации к системе управления информационной безопасности, необходимо подробно познакомится с данным понятием. При обсуждении ISO 27001 мы столкнёмся с понятием аудит. В настоящее время все более востребованной на рынке информационной безопасности становится услуга аудита. Однако, как показывает практика, и заказчики, и поставщики зачастую понимают суть этой услуги по-разному. Данная глава дает подробную классификацию услуг аудита и акцентирует внимание на особенностях различных видов аудита.

**Активный аудит**

Активный аудит является одним из самых распространённых видов аудита. Данный аудит является исследованием защищенности информационной системы предприятия с точки зрения хакера. Другими словами данный вид аудита можно назвать, как инструментальный анализ защищенности. Суть активного аудита заключается в том, что при помощи специализированного программного обеспечения происходит сбор информации о состоянии защиты. Стоит отметить тот факт, что под состоянием защиты понимаются только те настройки, с помощью которых злоумышленник может проникнуть в информационную систему.

Когда используется данный вид аудита, происходит моделирование огромного количества атак, которые может осуществить хакер для проникновения в информационную базу предприятия. Аудитор в это время становится хакером - ему предоставляется абсолютный минимум информации. Ему доступна только та информация, которую можно узнать из открытых источников.

Результатом такого аудита может служить информация о, различного рода уязвимостей в системе и способах ее устранения. По окончании активного аудита выдаются рекомендации по модернизации системы сетевой защиты. Они помогают устранить опасные уязвимости, повысив уровень защищенности информационной системы от действий «внешнего» злоумышленника при минимальных затратах на информационную безопасность.

Требуется проведения и других типов аудита для создания «идеальной» системы сетевой защиты. Активный аудит не предоставляет информации

корректности, с точки зрения безопасности, проекта информационной системы.

Под активным аудитом понимается услуга, которая может и должна заказываться периодически. Выполнения такого рода аудита должна проводиться раз в год, что позволит предприятию удостовериться, что в высоком уровне сетевой информационной безопасности.

Активный аудит условно можно разделить на два вида – «внешний» и «внутренний».

При «внешнем» активном аудите специалисты моделируют действия «внешнего» злоумышленника. В данном случае проводятся следующие процедуры:

* «Определение доступных сетей IP-адресов заказчика;
* Сканирование данных адресов с целью определения работающих сервисов и служб, а также назначения отсканированных хостов;
* Определение версий сервисов и служб сканируемых хостов;
* Изучение маршрутов прохождения трафика к хостам заказчика;
* Сбор информации об ИС заказчика из открытых источников;
* Анализ полученных данных с целью выявления уязвимостей».[[20]](#footnote-20)

«Внутренний» активный аудит по составу работ аналогичен «внешнему», однако есть отличие. При проведении такого рода аудита, хакер предоставляется как внутренний злоумышленник.

**Экспертный аудит**

Мной было выделено следующее определение экспертного аудита. Экспертный аудит – это сравнение состояния информационной безопасности с описание «идеала», базирующееся на следующем:

* Требования руководства при проведении аудита;
* Описание «идеала» информационной безопасности, основанной на частном опыте.

При проведении экспертного аудита, аудиторам необходимо сделать следующее:

• «Сбор исходных данных об информационной системе, об ее функциях и особенностях, используемых технологиях автоматизированной обработки и передачи данных (с учетом ближайших перспектив развития);

• Сбор информации об имеющихся организационно-распорядительных документах по обеспечению информационной безопасности и их анализ;

• Определение точек ответственности систем, устройств и серверов ИС;

• Формирование перечня подсистем каждого подразделения компании с категорированием критичной информации и схемами информационных потоков». [[21]](#footnote-21)

Самой объемной и трудоемкой работой всего аудита является сбор данных об информационной системе при помощи интервьюирования сотрудников компании. Основная цель интервьюирования технических специалистов – сбор информации о функционировании сети, а у руководящего состава компании – выяснение требований, которые предъявляются к системе информационной безопасности.

Основным этапом экспертного аудита является анализ информационной системы, топологии сети и способе обработки информации, при котором может выявиться снижения уровня защищенности информационной системы. По истечении данного этапа представляются документы, описывающие недостатки информационной системы с выделением критериев и способов увеличения уровня безопасности.

Следующим этапом является анализ информационных потоков организации.

На данном процессе происходит анализ информационных потоков ИС. Для уточнения процесса, также строятся различные диаграммы, которые показывают и определяют уровень защиты данного потока. После данного этапа работ аудиторами предлагается повышение уровня защищенности для ценной информации. Для неценной информации уровень защищенности остается прежним.

В процессе экспертного аудита проводится анализ организационно-распорядительных документов, таких как политика безопасности, план защиты и различного рода инструкции.

Определение полномочий и ответственности конкретных лиц за обеспечение информационной безопасности различных участков/подсистем ИС является важным шагом при анализе информационных систем. Полномочия и ответственность должны быть закреплены положениями организационно-распорядительных документов.

Типичный отчет о проведении экспертного аудита может включать в себя следующее:

* «Изменения (если они требуются) в существующей топологии сети и технологии обработки информации;
* Рекомендации по выбору и применению систем защиты информации и других дополнительных специальных технических средств;
* Предложения по совершенствованию пакета организационно-распорядительных документов;
* Предложения по этапам создания системы информационной безопасности;
* Ориентировочные затраты на создание или совершенствование СОИБ (включая техническую поддержку и обучение персонала)».[[22]](#footnote-22)

**Аудит на соответствие стандартам**

Основной сутью данного аудита является формулирование целей в финансовой сфере. При проведении данного аудита происходит сравнение текущей информационной безопасности с описанием некой безопасности в одном из стандартов.

Отчет, который будет подготовлен после проведения данного аудита, должен включать в себя следующее:

* Уровень соответствия информационной системы текущим стандартам;
* Уровень, которому соответствует внутренние требования предприятия в области информационной безопасности;
* Количество и категории полученных несоответствий и замечаний;
* Рекомендации по построению или усовершенствованию системы, которая обеспечивает информационную безопасность предприятия, позволяющая привести текущую информационную безопасность в соответствие с рассматриваемым стандартом;
* Основные документы заказчика, необходимые для обеспечения информационной безопасности.[[23]](#footnote-23)

Примером стандартов, которые будут рассматриваться в качестве «идеальных» может послужить следующие стандарты:

* Отечественные стандарты:
* «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К);
* «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (ГОСТ Р ИСО/МЭК 15408-2002 или «Общие критерии»).
* Международные стандарты:
* ISO/IEC 17799 (ныне называется ISO 27002) - «Информационные технологии. Управление информационной безопасностью»;
* «WOT (Web of Trust) — бесплатная надстройка к браузеру, которая предупреждает интернет-пользователя во время поиска информации или совершения покупок о сайтах с низкой репутацией».[[24]](#footnote-24)

Теперь перейдем к выделению основных причин проведения данного аудита. Причины условно можно разделить по степени обязательности:

* Обязательная сертификация;
* Сертификация, вызванная некими объективными причинами;
* Сертификация, позволяющая в будущем принести больший доход компании;
* Сертификация по доброй воле.

Государственные организации обязаны проводить ежегодную аттестацию безопасности своей информационной системы. Однако существуют и организации, которые не обязаны проводить аттестацию своей ИС. Для таких компаний проведение аудита будет намного выгоднее. За услугами аудита, заказчик обращается в крупную компанию-интегратор, которая обладает высоким опытом.

В большинстве случаев компании проводят аудит только лишь для того, чтобы привлечь крупного клиента, предоставляя ему сертификат, который подтверждает высокий уровень информационной безопасности. В такой ситуации происходит проведение сертификации на соответствие тем стандартам, которые довольно важны для клиентов.

В заключение данной главы отметим, что при планировке проведения проверки информационной безопасности важно не только грамотно выбрать вид аудита, но и правильно выполнить исполнителя. Ведь данный выбор напрямую зависит от потребностей, возможностей и желаний компании

# 2.3 Информационные риски компании

При внедрении системы управления информационной безопасностью в организацию, для аудиторов камнем преткновения обычно является система управления рисками. В данной главе мы подробно познакомимся с понятием рисков, а также способами управления ими.

Специалисты информационной безопасности не могут прийти к консенсусу при вопросе управления рисками. Кто-то отрицает те или иные методы оценки рисков, другие отрицают целостность анализа и управления рисками в целом. Есть и специалисты, которые утверждают, что компания не достаточно времени уделяет объективному анализу активов компании, таких как репутация компании. Отдельный класс специалистов предлагают тратить на процедуру обеспечения информационной безопасности столько денег, сколько осталось в бюджете.

 Риски подразумевают под собой причинения какого – либо ущерба в тот или иной момент времени. Это может быть как прямой ущерб, так и косвенный. При прямом ущербе можно привести пример попадание молнии в один из зданий компании, либо обесценивания некоторых ценных бумаг. Косвенный ущерб обозначает тот факт, что компания не заключила контракт с какой-либо компанией и не получила возможной прибыли.

Для достижения любых целей, организация использует несколько категорий ресурсов, которые именуются активами. «Активы — это ресурсы, контролируемые компанией в результате прошлых событий, от которых компания ожидает экономической выгоды в будущем».[[25]](#footnote-25) Другими словами, актив это вся ценность организации, которая приносит ей доход. Существует несколько типов активов:

* Материальные;
* Финансовые;
* Людские;
* Информационные;
* Процессы.

Последний тип активов был определён из современных международных стандартов. Процесс - это агрегированный актив, который оперирует всеми другими активами компании для достижения бизнес целей.[[26]](#footnote-26) Среди других важных активов компании стоит выделить имидж и репутацию. Данные активы приносят доходы компании косвенным способом, привлекая клиентов, ведь репутация и имидж – это активы, обладающие широко распространяемой информацией. Одной из основных целей информационной безопасности является защита имиджа компании, так как под имиджем компании часто понимается конфиденциальная информация, которая при ее утечке, может обрушить экономику предприятия.

Нарушение безопасности предприятия может затронуть сразу несколько групп активов организации. Например, произошел сбой сервера. Данный инцидент негативно влияет на доступность различных приложений, как и у сотрудников компании, так и у клиентов. Все это приводит к дефициту работников на определенном участке в компании, вызывая потребность в оптимизации бизнес- процессов. Таким образом, сбой сервера может привести к потере имиджа компании.

Все активы довольно важны для предприятия. Однако каждая компания разделяет все группы активов на два типа:

* Основные активы;
* Вспомогательные активы.

Определение данных активов не составит особого труда, ведь основными активами, компания считает те активы, вокруг которых организован бизнес компании.

Например, компания занимается продажей квартир и дачных участков. Для такой организации основным активом может служить материальный актив. Среди вспомогательных активов сюда можно отнести людской.

Риски потери одного из основных активов могут привести к потере бизнеса в целом. По этой причине, руководство организации лично следит за его работоспособностью.

Так как управления рисками являются, для большинства компаний, не основным элементом управления бизнесом, в практике применяются три основных подхода управления рисками:

* Для некритичных систем;
* Для критичных систем;
* Бизнес компании построен вокруг информационных активов.

В случае с некритичными системами, когда информационные активы являются вспомогательными, а уровень информации низок, есть лишь минимальная необходимость в оценке рисков. Для таких организаций необходима лишь базовая защита информации, которая будет соответствовать нескольким стандартам информационной безопасности. Более того при оценке рисков по стандартам, стоит помнить об экономической целесообразности применения тех или иных стандартов для данной организации.

При наличии критичной системы в организации, когда информационные активы не являются основными, однако информация очень необходима для бизнес-процессов, атака на информационный актив может сильно повредить один из основных бизнес- процессов компании. В таких случаях необходима оценка рисков, уделяя при этом больше времени на отдельные критичные информационные системы, которые более всего могут поддаваться нападению хакера.

В том случае, когда бизнес компании построен вокруг информационных активов, они относятся к основным, что означает тот факт, что для оценки таких рисков необходимо применять формальных полный подход.

При выборе похода оценки рисков предприятия стоит также помнить об уровнях зрелости анализируемой компании. «Управление рисками ИБ представляет собой непрерывный процесс, обеспечивающий выявление, оценку и минимизацию рисков от реализации угроз информационной безопасности, направленных на активы организации».[[27]](#footnote-27) По степени зрелости организаций можно выделить некоторые из них, которые определены стандартами COBIT и другими:

* На начальном уровне осознание как таковое отсутствует, в организации предпринимаются фрагментарные меры по обеспечению ИБ, инициируемые и реализуемые ИТ специалистами под свою ответственность.
* На втором уровне в организации определена ответственность за ИБ, делаются попытки применения интегрированных решений с централизованным управлением и внедрения отдельных процессов управления ИБ.
* Третий уровень характеризуется применением процессного подхода к управлению ИБ, описанного в стандартах. Система управления ИБ становится настолько значимой для организации, что рассматриваться как необходимый составной элемент системы управления организацией. Однако полноценной системы управления ИБ еще не существует, т.к. отсутствует базовый элемент этой системы – процессы управления рисками.
* «Для организаций с наивысшей степенью осознания проблем ИБ характерно применение формализованного подхода к управлению рисками ИБ, отличающегося наличием документированных процессов планирования, реализации, мониторинга и совершенствования».[[28]](#footnote-28)

**Процессная модель управления рисками**

Недавно был принят британский стандарт BS 7799 Часть 3– Системы управления информационной безопасностью - Практические правила управления рисками информационной безопасности. Данный стандарт предоставляет рекомендации по оценке и управлению рисками компании, используя при этом процессную модель, которая используется в других стандартах управления информационной безопасностью.

Данная процессная модель включает в себя следующие группы процессов:

* Планирование;
* Реализация;
* Проверка;
* Действия.

Стоит отметить, что стандарт ISO 27001, описывает цикл управления информационной безопасностью, в то время как BS 7799 – 3 описываются процессы управления рисками информационной безопасности.

Процесс планирование подразумевает под собой оценку рисков, которая включает в себя инвентаризацию активов, составление профилей угроз и уязвимостей, а также предоставление оценки об эффективности мер против возможного ущерба.

На этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. Организация принимает одно из решений:

* Проигнорировать;
* Избежать;
* Передать;
* Минимизировать.

После этого производится и происходит процесс внедрения плана обработки рисков.

На следующем этапе происходит отслеживание механизмов контроля на их функционирование. Также контролируются факторы риска, такие как: активы, угрозы и уязвимости. Конечным шагом данного этапа является проведение аудитов.

На этапе действия, по результатам предыдущих шагов, выполняются необходимые корректирующие действия, которые могут включать в себя:

* Процесс оценивания величины рисков;
* Изменение политики и методологии оценки рисков;
* Изменение плана обработки рисков.

**Факторы риска**

При анализе рисков не стоит забывать и об анализе факторов риска для принятия правильных решений по обработке рисков. Факторы риска – это основные параметры при оценке рисков. Стоит выделить все параметры:

* Актив
* Ущерб
* Угроза
* Уязвимость
* Механизм контроля
* Размер среднегодовых потерь
* Возврат инвестиций

Каждая компания производит анализ и оценку данных факторов при помощи методологии исследуемой организации. Стоит отметить, что общий подход к анализу практически одинаковый.

Процесс оценки рисков состоит из двух фаз. В первой фазе, которая называется анализ рисков, необходимо проделать следующее:

* Узнать, что является основным активом компании;
* Узнать реальную ценность данного актива;
* Провести анализ угроз относительно данного актива;
* Провести анализ ущерба и других угроз в случае нарушения информационной безопасности основного актива;
* Узнать, как сильно уязвим бизнес при данных угрозах;
* Проанализировать среднегодовые потери.

Вторая фаза носит название оценивание рисков. После анализа рисков, аудиторы получают риски, которые превышают допустимый уровень. В данной фазе происходит процесс обработки риска, и проделываем следующее:

* Выбираем вариант обработки риска;
* Анализ механизмов контроля при минимизации риска;
* Анализ эффективности выбранных механизмов контроля и инвестиций.

После принятия решения по обработке рисков, для того, чтобы руководство могло принять правильное решение, ответственный за управление рисками в компании должен предоставить ему информацию. Данная информация должна включать в себя:

* Сообщение о проблеме. Источник проблемы и способ реализации;
* Степень серьезности проблемы. Возможные потери для предприятия;
* Предлагаемое решение. Анализ действий для исправления ситуации вместе с возможным финансовым планом на реализацию данного решения;
* Альтернативные решения. Предоставление других способов решения проблемы.

Эффективность процесса управления рисками ИБ определяется точностью и полнотой анализа и оценки факторов риска, а также эффективностью используемых в организации механизмов принятия управленческих решений и контроля их исполнения.

# 2.4 Применение и сбор требований системы менеджмента информационной безопасности, основанных на стандартах ISO 27001 и ISO 27002.

В данной главе будет произведен анализ требований менеджмента информационной безопасности на основе стандартов ISO 27001 и 27002 для российских предприятий. Перед выделением требований, хотелось бы проанализировать эти два стандарта.

Стандарт ISO 27001 включает в себя описание общей модели внедрения и функционирования системы менеджмента информационной безопасности. Цель данного стандарта заключается в обеспечении согласованности менеджмента ИБ вместе с другими системами управления в компании. Другими словами, это значит, что при внедрении других стандартов менеджмента, она может с легкостью применять единую систему аудита.

Система менеджмента информационной безопасности описана в данном стандарте с точки зрения создания, внедрения, эксплуатации, мониторинга и поддержки. При внедрении данной системы, компанию получает средства мониторинга и управления безопасностью, которые помогают снизить различные типы рисков.

В приложениях стандарта ISO 27001 содержаться цели и средства управления информационной безопасности. При внедрении системы менеджмента ИБ, стандарт ISO 27001 использует «цикл СМИБ».

В разделах четыре и восемь стандарта ISO 27001 содержатся основные требования создания СМИБ, который указан на рисунке семь.

Стандарт ISO 27002 «Свод правил по менеджменту информационной безопасности». «Стандарт предоставляет лучшие практические советы по менеджменту информационной безопасности для тех, кто отвечает за создание, реализацию или обслуживание систем менеджмента информационной безопасности».[[29]](#footnote-29) ISO 27002 не определяет, как нужно применять средства управления. Он предоставляет направление для создания системы менеджмента, которое позволяет выбрать средства управления.

В зависимости от технической и физической среды компании, руководство самостоятельно должно выбрать процедуры для внедрения.

Компания должна серьезно относиться к информационным активам, и внедрить СМИБ, основываясь на стандарте ISO 27002. Данный стандарт включает в себя двенадцать разделов, которые описывают средства управления безопасностью такие как:

* «Политика безопасности;
* Организация информационной безопасности;
* Управление ресурсами;
* Безопасность персонала;
* Физическая безопасность и безопасность окружения;
* Управление коммуникациями и операциями;
* Управление доступом;
* Приобретение, разработка и поддержка систем;
* Управление инцидентами информационной безопасности;
* Управление бесперебойной работой организации;
* Соответствие нормативным требованиям».[[30]](#footnote-30)

Стандарт ISO 27001 представляет систему менеджмента информационной безопасности. Стандарт ISO 27002 представляет руководящие принципы по реализации ресурсов управления.

Перейдем к обсуждению системы менеджмента информационной безопасности. На эффективность данной системы может влиять огромное количество различных факторов. Одним из таких факторов может являться риск-менеджмент, которые включает в себя следующие основные понятия:

* Организационная безопасность;
* Физическая безопасность;
* Безопасность персонала;
* Управление активами;
* Безопасность коммуникаций;
* Безопасность функционирования;
* Безопасность разработки и закупки информационных технологий;
* Обеспечение непрерывности бизнеса.

Каждый из разделов включает в себя большое количество подразделов. В качестве примера приведем раздел: управление доступом. Он может включать в себя подразделы: доступ на уровне пользователей, доступ на уровне компонентов операционной системы. В свою очередь каждый из компонентов может обладать своими особенностями, что приводит к сложностям. Для избегания этого необходимо разработать структуру, которая поможет избавиться от проблем. Это можно сделать с помощью системы менеджмента безопасности.

СМБ представлена в виде схемы, которая описывает основные разделы безопасности, состоящая из разделов и подразделов. Специалисты тщательно разрабатывают и описывают систему менеджмента безопасности, так как в будущем она будет неоднократно применяться. Стоит выделить одну из функций данной системы. Она позволяет:

* Отслеживать ход разработки;
* Отслеживать ход внедрения;
* Отслеживать эффективность политики, процедур и стандартов, которые принимаются для каждого из разделов безопасности.

Данные элементы также могут быть использованы компанией для контроля поставщиков услуг. При этом данные услуги могут быть разными и варьироваться от внутренних до услуг, переданных на аутсорсинг. СМБ позволяет выделить некие границы документации и инструментарий, который регулирует соответствие. Среди инструментария стоит выделить следующие элементы:

* Опросники;
* Аналитические инструменты;
* Инструменты для создания отчетов;
* Инструменты для отслеживания работ по устранению недостатков.

Формальное и грамотное построение системы менеджмента информационной безопасности позволить получить отдачу от инвестиций в обеспечение безопасности компании. Это может быть достигнуто путем снижения бизнес – рисков, а именно уменьшения штрафов, которые накладываются на компанию. Многие требования безопасности могут трактоваться по-разному, поэтому необходимо разработать некий документ, где будут предоставлены все требования, необходимые для реализации системы менеджмента информационной безопасности.

В России существует только один единый документ, который описывает цели и задачи обеспечения информационной безопасности Российской Федерации, утвержденный В.В. Путиным. Однако данный документ рассматривает общие черты предоставление ИБ, среди которых:

* «Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.
* Информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.
* Развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов».[[31]](#footnote-31)

На основе данной доктрины сложно внедрить СМИБ на российское предприятие. В данном дипломе были предоставлены требования, которые необходимы для внедрения системы менеджмента информационной безопасности, основанные на стандартах ISO 27001 и ISO 27002. Проанализировав два стандарта, в данной работе было выделено двенадцать основных разделов СМБ, которые включают в себя подразделы:

* Политика безопасности;
* План менеджмента безопасности;
* Управления активами;
* Безопасность персонала;
* Физическая безопасность;
* Безопасность активов;
* Управление эксплуатацией;
* Управление доступом;
* Обеспечение качества, принятых решений;
* Управление инцидентами;
* Непрерывность бизнеса;
* Управление соответствием и аудитом.

Перейдем к описанию каждого из элементов.

**Политика безопасности.**

* Политика безопасности информации.
* Документация;
* Знакомство с политикой;
* Просмотр и пересмотр политики.

Наличие политики безопасности компании является обязательным требованием для обеспечения защиты информации. Под политикой компании подразумевается свод требований, которым должно соответствовать предприятие, поддерживающее миссию компании. Документация подразумевает создание руководством четких вопросов по управлению информационной безопасностью, а также правила их реализации. Все сотрудники должны быть ознакомлены с политикой компании. Россия не имеет типового документа по политике безопасности. В британском стандарте BS7799:1995 указаны пункты, которые необходимо включить в политику ИБ.

* Вводный документ. Данный документ должен подтверждать заинтересованность высшего руководства по обеспечению информационной безопасности;
* Организационный документ. Данный документ описывает подразделения, комиссии и группы, которые отвечают за ту или иную работу в информационной безопасности;
* Классификационный документ. Данный документ описывае, имеющиеся на предприятии ресурсы и необходимый уровень их защиты;
* Документ физической защиты информации;
* Документ, описывающий правила разграничения доступа к информации на предприятии;
* Документ описания и порядка внедрения различных информационных систем на предприятие.

 В случае каких-либо изменений в структуре компании или по истечению какого-либо определенного времени, требуется тщательный пересмотр политики компании на соответствие и соблюдение всех указанных в ней рекомендаций.

**План менеджмента безопасности.**

* Участие высшего и среднего руководства в обеспечении безопасности;
* Согласованность информационной безопасности;
* Определение ролей и обязанностей в менеджменте безопасности;
* Процесс авторизации и аутентификации;
* Конфиденциальность;
* Внешние организации;
* Аудит.

План менеджмента безопасности описывает требования к основным понятиям безопасности. Необходимо участие руководства, а именно стратегическое управление для успешной реализации программы. Определение бизнес – рисков компании и надзор за предотвращением таковых является функцией руководства. При внедрении безопасности необходима сплоченность всех департаментов компании в группе внедрения безопасности для бизнес-планирования и анализа. Четкое определение ролей и обязанностей по стратегическому управлению и обеспечению безопасности является следующим обязательным разделом. Установление единой политики на средства по обработки данными или организация управления учеными записями пользователей, которая применяется к физическому или к виртуальному доступу. Сотрудники компании должны иметь представления о своих обязанностях и возлагаемой на них ответственности. На основании этого, руководство имеет законные основания, не нарушая прав своих сотрудников, применять действия по обеспечению безопасности предприятия. Руководство должно быть подготовлено к чрезвычайным ситуациям и обладать политикой, при которой организация определяет к каким органам стоит обращаться в случае возникновения той или иной ситуации. Требуется провести независимый аудит сторонней организацией, несмотря на профессионализм специалистов. Это должно проходит каждый определенный промежуток времени, установленный компанией.

Упрощенный план менеджмента безопасности должен быть представлен в виде документа со следующими полями:

* Фаза;
* Менеджер проекта;
* Поставщик;
* Ответственный за систему;
* Внешний или внутренний оценщик;
* Внешняя или внутренняя структура безопасности.

**Управление активами.**

* Ответственность за активы;
* Инвентаризация;
* Определение владельца;
* Политика использования;
* Классификация информации;
* Классификация;
* Обращение с информацией.

Управление активами— профессиональное управление различными типами ценных бумаг (акциями, облигациями и т. д.) и другими активами (например, недвижимостью), целью которого является получение прибыли инвесторами. «Инвесторами в данном случае могут выступать как компании (страховые компании, пенсионные фонды, корпорации и т. д.), так и частные инвесторы (непосредственно или с помощью коллективного инвестирования)».[[32]](#footnote-32) Инвентаризация подразумевает под собой идентификацию всех активов компании с последующим указанием важности каждого из активов. Оценка критичности активов выполняется по трем параметрам: конфиденциальности, целостности и доступности. Т.е. следует оценить ущерб, который понесет компания при нарушении конфиденциальности, целостности или доступности активов. Также стоит выделить некую методологию мониторинга активов, в случае возникновения рисков. За каждым активом должен быть закреплен владелец, который будет распределять права доступа к нему вместе с пользованием. Владельцы активов должны руководствоваться некой политикой, которой они должны следовать при управлении активами. Раздел «управление активами» включает в себя подраздел классификация информации, который указывает на требования для сохранения информации об активах. Требуется разработка классификации информации для эффективного управления рисками. Владелец активов сам производит классификацию и соблюдает данные требования для всей информации, чтобы произвести защиту активов. Также необходима инструкция по обращению с любой информацией, располагаемой в компании в зависимости от ее классификации.

**Безопасность персонала**

* Соблюдение безопасности для сотрудников перед приемом на работу;
* Роли и обязанности;
* Проверка предоставленной информации;
* Соблюдение законодательных требований;
* Соблюдение безопасности для сотрудников во время их работы;
* Осведомленность сотрудников;
* Обучение и тренинги;
* Наказания.

При внедрении системы безопасности на предприятие огромное внимание уделяется обеспечению безопасности людских ресурсов. Необходимо выделить роли и обязанности, связанные с безопасностью, а затем назначит кадровую службу, которая будет вести учет данных ролей. Перед приемом сотрудника на работу требуется тщательно проанализировать, предоставленную им информацию на наличие ошибок и возможной недосказанности. Заключение сотрудничества на основе договора, имеющего юридическую силу.

Данный раздел включает в себя подраздел, который описывает некоторые требования, необходимые для соблюдения безопасности сотрудника и компании во время работы. Каждый сотрудник должен знать свои обязанности и свою роль в соблюдении политики безопасности компании. Компания должна проводить тренинги по повышению работоспособности и осведомленности сотрудников относительно безопасности. Обучение сотрудников должно обеспечить знание ими требований безопасности, ответственности в соответствии с законодательством, мероприятий по управлению информационной безопасностью, а также знание правильного использования средств обработки информации, например процедур регистрации в системах, использования пакетов программ, прежде чем им будет предоставлен доступ к информации или услугам. Все пользователи должны быть обязаны сообщать определенным лицам об инцидентах и слабых местах в системе безопасности, сбоях в работе программного и аппаратного обеспечения. Необходимо определить и довести до сведения пользователей методы фиксации симптомов сбоев оборудования. Необходимо обеспечивать защиту персональных данных. Необходимо назначить ответственное лицо за обеспечение безопасности персональных данных. Нужно соблюдать «правило чистого рабочего стола», которое требует от пользователя регулярную чистку файлов, связанных с паролями на компьютере. Должны быть установлены санкции за нарушение политики менеджмента безопасности.

**Физическая безопасность.**

* Расположение;
* Политика входа и выхода;
* Безопасность офисов;
* Внешние угрозы;
* Области с повышенной опасностью.

Обеспечение физической безопасности является главным аспектом безопасности, так как при несоблюдении этой политики можно пострадать физически. В зависимости от территории, в которой находится предприятие, требуется соблюдение политик безопасности. Для уменьшения затрат, требуется ограничить число входов и выходов каждого пользователя в систему. Следует скрывать различные помещения, требуемые специальной степени защиты. Необходимо прописать политики в случае природных катаклизм и технологических аварий, связанных с жизнью человека. Требуется описание политик для мест, которые требуют повышенной меры безопасности.

**Безопасность активов.**

* Меры;
* Сопровождение;
* Использование активов;
* Уничтожение актива;

Необходимо физическое ограничение доступа защищаемых помещений или технических средств, чтобы злоумышленник не смог увидеть или проникнуть к активам. При внедрении той или иной системы, например CRM, необходимо не только умение пользование данной системой, но и оказание услуг, системы консалтинга, которая внедрила эту систему. Нужно поддерживать и сопровождать внедренные системы. После обновления того или иного актива и передачи его другому лицу, нужно тщательно удалить всю информацию, связанную с этим активом. Примером может служить передача компьютера руководителя бухгалтеру. Установите стандарты и правила, по которым стоит удалять актив. Следует проводить мониторинг соблюдения введенных стандартов для качественного обеспечения безопасности предприятия.

**Управление эксплуатацией.**

* Работоспособность;
* Управление тестированием;
* Управления логами (журналами событий).

Под понятием работоспособности системы я, на основе проведенных исследований, подразумеваю поддержание системы в рабочем состоянии, несмотря на внешние и внутренние воздействия, благодаря системам восстановления, системам защиты от несанкционированного доступа (НСД) и системам обслуживания.

Необходимо разработать документацию по работе с информационными технологиями на предприятии и выделить основные процедуры, такие как: включение системы, обслуживание, восстановление, пронос данных, шифрование. При нехватке каких-либо знаний в том или ином департаменте, необходимо временно перевести сотрудника в данный отдел для отсутствия прерывания бизнес- процесса компании. Для предотвращения попадания ненужных элементов в среду разработки, необходима аналогичная система, которая поможет ИТ – специалистам проводить тестирование различных элементов, без остановки рабочей системы. Примером такой системы может служить salesforce.com. В наличии данной системы имеется версия Production- рабочая система предприятия, а также sandbox – «песочница», предназначенная для тестирования отдельных объектов, полей, бизнес-правил предприятия. Утверждение политики ведения журналов поможет компании отслеживать изменения записей, относящихся к продажам, сотрудникам и другим ресурсам. Данное отслеживание может быть осуществлено с помощью уведомлений на электронную почту руководства.

**Управление доступом.**

* Управление учетными записями;
* Управление дополнительными возможностями пользователей;
* Пересмотр возможностей пользователя;
* Классификация информации.

Необходимо разработать процесс регистрации, аутентификации и входа пользователя в систему. Примером может служить система salesforce.com. При создании пользователя можно задать определенное бизнес – правило, которое будет отправлять уведомление на почту руководителю, который должен утвердить данный контакт или любое другое поле на предприятии. Каждый пользователь системы должен обладать своими привилегиями. Для этого необходимо разработать иерархию ролей компании в системе и предоставлять доступ к определенной информации пользователям, которые занимают ту или иную роль в компании. Предоставление привилегий проводится администраторами, таким образом, они должны каждый промежуток времени сверять настройки пользователя на наличие ошибок и в случае нахождения таковых, немедленно исправлять. При отсутствие данной процедуры пользователю может быть доступна ненужная ему информация о компании, которую он может по ошибке изменить. Необходимо классифицировать информацию, которая будет доступна каждому профилю пользователей.

**Обеспечение качества принятых решений.**

* Безопасность информационных технологий;
* Точность информации;
* Безопасность файлов;
* Управление уязвимостями;

Необходимо создать требования, необходимые для обеспечения безопасности ИТ. Данные требования создаются индивидуально, в зависимости от предоставляемых услуг компанией. Необходимо быть уверенным в предоставлении точной информации без «мусора», а также ее отправке. Для этого необходимы сторонние приложения, такие как антивирусные системы, через которые будет проходить поток информации, который будет сверяться и в случаи ошибки редактироваться. Необходимо правильное разделение полей доступа в базе данных предприятия, для безопасности файлов. Это подразумевает наличие отдельных сред, где каждая группа пользователей будет работать обособленно друг от друга. При соблюдении данных правил, ИТ специалисты смогут редактировать систему, не мешая менеджерам или операторам кол-центра выполнять свои обязанности, тем самым не нарушая общие правила бизнес-процесса. Управление уязвимостями, обозначает наличие документа для руководства, где будут описаны все уязвимости программных и аппаратных средств предприятия. ИТ-специалисты необходимы, принимать участие в разработке патчей для ликвидации возможных багов, уязвимостей компании.

**Управление инцидентами.**

* Выявление;
* Уведомление;
* Действие.

Необходимо создание политики для обеспечения выявления инцидентов на предприятии. Например, автоматический мониторинг каждую единицу времени на определенных секторах. Для того, чтобы выявленный инцидент не смог нарушить бизнес-процессы, необходимо вовремя уведомить об этом сотрудников. Чаще всего для этого внедряется департамент Help Desk(техническая поддержка), которая занимается процессом уведомления. Также данный департамент занимается подразделом «дейтсвие» данной рекомендации. Техническая поддержка обязана не только уведомить весь персонал об инциденте, но и сделать все возможное для его ликвидации. В случае невозможности ликвидации, Help Desk должен обратиться в сторонние службы для оказания помощи.

**Непрерывность бизнеса.**

* Управление непрерывностью бизнеса;
* Оценка угроз;
* Оценка рисков;
* Сопровождение непрерывности бизнеса.

Необходимо использовать оценку угроз и рисков для четкого управления непрерывность бизнеса. Должна быть разработана политика восстановления бизнеса компании после того или иного инцидента. Необходимо спланировать возможные угрозы предприятия и оценить возможный ущерб. Необходимо определить основный актив компании и выделить вероятность риска, которая понесет за собой возможный ущерб. Подробная информация об оценке рисков описана в главе 2.3. Необходимо разработать план по восстановления работоспособности информационной системы компании для продолжения ведения бизнеса, с минимальными затратами. В программной среде salesforce.com эта функция реализуется с помощью неких событий-триггеров, которые являются генератором ошибок системы, не позволяющие привести к ошибке в системе предприятия.

**Управление соответствием и аудитом.**

* Стандарты и кодекс
* Защита данных;
* Аудит безопасности;
* Инструменты аудита.

Необходимо создание общих списка всех, относящихся к компании требований на основе кодекса и различных стандартов. Это необходимо для того, чтобы выделить какими ресурсами и программным обеспечением необходимо пользоваться для соблюдения законности. Необходимо создать политику защиты данных, в которой будет обговорены пределы выноса информации за пределы организации, а также количество и тип возможной выносимой информации. Должен проводиться аудит средств безопасности для обеспечения уверенности руководства в том, что компания хорошо защищена. Он, должен быть осуществлен каждый определенный промежуток времени, сторонней аудиторской компанией. Внутри компании необходимо наличие сотрудника, который будет отвечать за использование программного средства на наличие уязвимостей в системе, с последующей ее ликвидацией. Нужно ограничить доступ к данному программному средству от неуполномоченных лиц для предотвращения нанесения вреда компании.

Внедрение системы менеджмента информационной безопасности – процесс довольно трудоемкий. Однако при соблюдении данных рекомендаций процесс внедрения окажется быстрым, а защита предприятия довольно эффективная.

##

## Заключение

Таким образом, в данной дипломной работе был дана характеристика информационной безопасности, а также различные теоретические аспекты менеджмента информационной безопасности, понятие рисков и активов компании, необходимые для полного понятия системы внедрения. Был проведен анализ и сравнительная характеристика отечественных и международных стандартов с дальнейшим выделением плюсов и минусов, которые существенно повлияли на практическую часть данной работы.

На основе полученного анализа были созданы соответствующие рекомендации, необходимые для минимальной защиты российского предприятия от угроз информационной безопасности. Внедрив систему менеджмента информационной безопасности на основе созданных рекомендаций, компания может достигнуть существенных изменений в конкурентоспособности, как по защите, так и по прибыльности своего бизнеса.

## Список литературы

1. [http://ru.wikipedia.org/wiki/Кофиденциальность](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C)
2. [http://ru.wikipedia.org/wiki/Целостность\_информации](http://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8)
3. [http://ru.wikipedia.org/wiki/Авторизация](http://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F)
4. <http://www.comss.ru/page.php?id=1398> – Статья - «VB100 Апрель 2013: Сравнительное тестирование антивирусов»
5. <http://www.razgovorodele.ru/security1/safety05/technician04.php> - Статья - «Основные направления информационной безопасности»
6. <http://ru.wikipedia.org/wiki/ISO/IEC_27001>
7. <http://www.complexdoc.ru/>
8. <http://sp-egov.ru/blog/chapter5/s51> - Статья - «Инфраструктура обеспечения юридической значимости электронного взаимодействия»
9. <http://www.ekey.ru/company/dictionary>
10. [http://ru.wikipedia.org/wiki/Критерии\_определения\_безопаности\_компьютерных\_систем](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D1%82%D0%B5%D1%80%D0%B8%D0%B8_%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D1%85_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC)
11. [http://ru.wikipedia.org/wiki/WOT:\_Web\_of\_Trust](http://ru.wikipedia.org/wiki/WOT%3A_Web_of_Trust)
12. <http://bugtraq.ru/library/security/practicaliso.html> - Статья - «Практические аспекты применения международного стандарта безопасности информационных систем ISO 27001:2005»
13. [http://ru.wikipedia.org/wiki/Актив](http://ru.wikipedia.org/wiki/%D0%90%D0%BA%D1%82%D0%B8%D0%B2)
14. <http://www.cnews.ru/reviews/index.shtml?2006/11/24/218588> - статья «Внедрение СУИБ: как управлять рисками? »
15. <http://www.pointlane.ru/process/risks/>
16. <http://ru.wikipedia.org/wiki/ISO/IEC_27002>
17. http://ru.wikipedia.org/wiki/Управление\_активами
18. Указ Президента РФ от 06.03.1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера»
19. Ведущий специалист ЗАО «АНДЭК» Роман Просянников Журнал «Connect», статья «Виды аудита информационной безопасности»
20. Чумарин Игорь «Тайна предприятия: что и как защищать»
21. Статья 139 ГК РФ «Служебная и коммерческая тайна»
22. Статья 183 УК «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну
23. Статья 147 УК «Нарушение изобретательских и патентных прав»
24. Статья 857 УК «Банковская тайна»
25. Т. А. Ми шов а, С. А. Охрименко, С. А. Тутунару, К. Ф. Склифос «О некоторых особенностях подготовки специалистов в области информационной безопасности для успешного ведения бизнеса»
26. ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»
27. Государственный стандарт РФ ГОСТ Р ИСО/МЭК 15408-2-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
28. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»
29. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»
30. ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
31. ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»
32. Серия международных стандартов ISO 27000
33. Александр Астахов «Искусство управления информационными рисками»

# Приложение 1

Защита информационной безопасности



Рисунок 1: Рейтинг антивирусов Virus Bulletin 2013, Февраль



Рисунок 2: Цели использования сетевых экранов

# Приложение 2

Атаки на информационную систему



Рисунок 3: Классификация атак



Рисунок 4: Типичный интерфейс Аномайзера

# Приложение 3

Управление рисками



Рисунок 5: Процессная модель

# Приложение 4

Система менеджмента информационной безопасности



Рисунок 6: Цикл СМИБ

1. Указ Президента РФ от 06.03.1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера» [↑](#footnote-ref-1)
2. ФЗ № 98 «О коммерческой тайне» [↑](#footnote-ref-2)
3. Статья 183 УК «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» [↑](#footnote-ref-3)
4. Чумарин Игорь «Тайна предприятия: что и как защищать» [↑](#footnote-ref-4)
5. Статья 147 УК «Нарушение изобретательских и патентных прав» [↑](#footnote-ref-5)
6. Статья 857 УК «Банковская тайна» [↑](#footnote-ref-6)
7. Там же [↑](#footnote-ref-7)
8. http://ru.wikipedia.org/wiki/Кофиденциальность [↑](#footnote-ref-8)
9. http://ru.wikipedia.org/wiki/Целостность\_информации [↑](#footnote-ref-9)
10. Т. А. Ми шов а, С. А. Охрименко, С. А. Тутунару, К. Ф. Склифос - Статья «О некоторых особенностях подготовки специалистов в области информационной безопасности для успешного ведения бизнеса» [↑](#footnote-ref-10)
11. Т. А. Ми шов а, С. А. Охрименко, С. А. Тутунару, К. Ф. Склифос – там же. [↑](#footnote-ref-11)
12. http://ru.wikipedia.org/wiki/Авторизация [↑](#footnote-ref-12)
13. Т. А. Ми шов а, С. А. Охрименко, С. А. Тутунару, К. Ф. Склифос – там же. [↑](#footnote-ref-13)
14. http://www.razgovorodele.ru/security1/safety05/technician04.php [↑](#footnote-ref-14)
15. Там же [↑](#footnote-ref-15)
16. http://ru.wikipedia.org/wiki/ISO/IEC\_27001 [↑](#footnote-ref-16)
17. http://sp-egov.ru/blog/chapter5/s51 - Статья - «Инфраструктура обеспечения юридической значимости электронного взаимодействия» [↑](#footnote-ref-17)
18. http://www.ekey.ru/company/dictionary [↑](#footnote-ref-18)
19. ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» [↑](#footnote-ref-19)
20. Просянников Роман Журнал «Connect», статья «Виды аудита информационной безопасности», ведущий специалист ЗАО «АНДЭК» [↑](#footnote-ref-20)
21. Там же [↑](#footnote-ref-21)
22. Просянников Роман Журнал «Connect», статья «Виды аудита информационной безопасности», ведущий специалист ЗАО «АНДЭК» [↑](#footnote-ref-22)
23. Там же [↑](#footnote-ref-23)
24. http://ru.wikipedia.org/wiki/WOT:\_Web\_of\_Trust [↑](#footnote-ref-24)
25. http://ru.wikipedia.org/wiki/Актив [↑](#footnote-ref-25)
26. http://www.cnews.ru/reviews/index.shtml?2006/11/24/218588 - статья «Внедрение СУИБ: как управлять рисками? » [↑](#footnote-ref-26)
27. http://www.pointlane.ru/process/risks/ [↑](#footnote-ref-27)
28. http://www.cnews.ru/reviews/index.shtml?2006/11/24/218588 - статья «Внедрение СУИБ: как управлять рисками? » [↑](#footnote-ref-28)
29. http://ru.wikipedia.org/wiki/ISO/IEC\_27002 [↑](#footnote-ref-29)
30. [там](http://ru.wikipedia.org/wiki/ISO/IEC_27002) же [↑](#footnote-ref-30)
31. Доктрина информационной безопасности Российской федерации [↑](#footnote-ref-31)
32. http://ru.wikipedia.org/wiki/Управление\_активами [↑](#footnote-ref-32)