УТВЕРЖДАЮ

" ___ " _____ 2018 г

СТО № ИБ.004

Система управления и обеспечения информационной безопасности в ООО «Сатурн»

Версия 1.0

Москва
2018

Сведения о нормативном документе

Информация о документе	
Функциональный руководитель	
Разработчик документа	
Введен в действие	Приказом № _____ от ___.___._____
Срок действия	не ограничен

История изменений			
Дата	**Версия**	**Автор изменений**	**Причина внесения изменений**

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

Практически все бизнес-процессы Компании используют информационные технологии и становятся зависимыми от их безопасности. В результате возникновения инцидентов информационной безопасности (реализации угроз) может быть нарушена работа информационных систем, что может привести к прерыванию бизнес-процессов и повлечь возникновение ущерба для Компании, который может быть оценен, например, в финансовом выражении или в виде ущерба репутации.

Основными целями настоящего стандарта являются:

- Стандартизация подхода к управлению и обеспечению информационной безопасности в Компании;
- Формирование механизма для оценки уровня информационной безопасности Компании;
- Создание механизма для формирования стратегии развития ИБ Компании;
- Достижение адекватности используемых защитных мер рискам ИБ.

2 ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт является нормативным документом Компании и распространяется на все компоненты инфраструктуры, в рамках которых обрабатывается конфиденциальная информация, такая как: персональные данные, инсайдерская информация и коммерческая тайна, а также процессы обеспечения безопасности такой информации.

Настоящий стандарт не распространяется на компоненты инфраструктуры и бизнес-процессы, в рамках которых обрабатывается информация, относящаяся к государственной тайне РФ.

Требования настоящего стандарта относятся к двум категориям: «Обязательные» и «Рекомендованные». «Обязательные» требования - должны неукоснительно выполняться в Компании, «Рекомендованные» - применяются по решению Компании.

3 НОРМАТИВНЫЕ ССЫЛКИ

«Корпоративный стандарт ИБ Компании разработан с учетом требований и рекомендаций следующих нормативно-правовых актов РФ, а также российских и международных стандартов области ИБ:

- Федеральный закон РФ «О персональных данных», N 152-ФЗ от 27.07.2006.
- Федеральный закон РФ «О коммерческой тайне», N 98-ФЗ от 29.07.2004.
- Федеральный закон РФ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» N 224-ФЗ от 27.07.2010.
- Закон РФ «О государственной тайне», N 5485-1 от 21.07.1993.
- Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», СТО БР ИББС-1.0-2014 от 01.06.2014.
- Международный стандарт ISO/IEC 27001:2013.
- Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», №687 от 15.09.2008.
- Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», №1119 от 01.11.2012.

- Приказ Федеральной службы по техническому и экспортному контролю «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», №21 от 18.02.2013.
- Приказ ФСБ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», №378 от 10.07.2014.

В Стандарте учтены требования следующих внутренних нормативных документов Компании:

- Кодекс «Безопасность».
- Кодекс «Материально-техническое и информационное обеспечение».
- Кодекс «Риски».
- «Положение о Подкомитете по рискам при Комитете по финансам и инвестициям», приложение к приказу Президента №У-070/09 от 04.06.2009.
- Кодекс «Управление персоналом».

Настоящий Стандарт ссылается на следующие внутренние нормативные документы Компании:

- «Корпоративная методика проведения аудита ИБ Компании.
- «Корпоративный регламент проведения аудита ИБ Компании.

4 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Активы. Под активами понимаются ресурсы Компании, в том числе:

- Информационные активы, в том числе представленные в виде баз и файлов данных, а также документов на бумажном носителе.
- Аппаратные активы (аппаратные ИТ-ресурсы), в том числе сетевое оборудование, серверы, рабочие станции, оргтехника и носители данных, содержащие конфиденциальную информацию.
- Программные активы.
- Помещения.
- Каналы и средства связи.

Внешние стороны - сторонние организации (третьи лица), которые могут повлиять на безопасность данных Компании или работоспособность сервисов и информационных систем. Например, это могут быть организации, предоставляющие Компании техническую поддержку или иные ИТ-сервисы, а также организации, имеющие доступ к ресурсам корпоративной сети Компании или к данным Компании.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-

розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
(Закон РФ N 5485-1 от 21.07.1993)

Допустимая точка восстановления (RPO) – точка во времени до начала инцидента, на момент которой должны быть восстановлены данные в информационной системе после завершения инцидента.

Допустимое время восстановления (RTO) – точка во времени, после начала инцидента, характеризующая максимально допустимое время простоя сервиса.

Инсайдерская информация – точная и конкретная информация, которая не была распространена или предоставлена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну), распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров и которая относится к информации, включенной в соответствующий перечень инсайдерской информации;
(Федеральный закон РФ N 224-ФЗ от 27.07.2010)

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.
(Федеральный закон РФ N 98-ФЗ от 29.07.2004, Кодекс «Безопасность» Компании)

Мобильные устройства - личные и корпоративные переносные средства вычислительной техники, используемые для доступа к ресурсам сети компании. Например: ноутбуки, мобильные телефоны, планшеты.

Мониторинг событий ИБ - процесс просмотра и анализа журналов зарегистрированных событий информационных систем, средств защиты информации и сетевых устройств Компании, проводимый с целью выявления инцидентов ИБ и их регистрации.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.
(Федеральный закон РФ N 152-ФЗ от 27.07.2006, Кодекс «Безопасность» Компании)

5 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

DLP	Система защиты от утечек данных

DMZ	Демилитаризованная зона
VPN	Virtual Private Network — виртуальная частная сеть
ИБ	Информационная безопасность
ИИ	Инсайдерская информация
ИКТ	Информация, составляющая коммерческую тайну
ИС	Информационная система
ИСПДн	Информационная система персональных данных
ИТ	Информационные технологии
Компания	Компании
ЛВС	Локальная вычислительная сеть
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
РФ	Российская Федерация
СКЗИ	Система криптографической защиты информации
СУБД	Система управления базами данных
СУИБ	Система управления информационной безопасностью
ТЗ	Техническое задание
ФСБ	Федеральная служба безопасности Российской Федерации

6 КОРПОРАТИВНЫЕ ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1 Классификация корпоративных требований по информационной безопасности

Каждому корпоративному требованию по ИБ соответствует определенный частный показатель ИБ. Все частные показатели ИБ объединены в 27 групповых показателей, в свою очередь объединенных в 2 направления:

К направлению «Обеспечение ИБ» относятся следующие групповые показатели:

1.1 Обеспечение информационной безопасности при работе с внешними сторонами.
1.2 Обеспечение информационной безопасности при управлении персоналом.
1.3 Обеспечение информационной безопасности при работе с мобильными устройствами, используемыми для доступа к ресурсам корпоративной сети, и носителями информации.
1.4 Обеспечение информационной безопасности на стадиях жизненного цикла информационных систем.
1.5 Обеспечение антивирусной защиты.
1.6 Безопасность сети и сетевого доступа.
1.7 Регистрация и мониторинг событий информационной безопасности.
1.8 Управление доступом и парольная защита.
1.9 Безопасность удаленного доступа.
1.10 Криптографическая защита информации и управление криптографическими ключами.
1.11 Резервирование и резервное копирование.
1.12 Управление техническими уязвимостями и безопасная конфигурация.
1.13 Защита от утечек конфиденциальной информации.
1.14 Защита персональных данных.
1.15 Защита коммерческой тайны.

К направлению «Управление ИБ» относятся следующие групповые показатели:

2.1 Документирование и управление документацией.
2.2 Распределение ответственности.
2.3 Управление активами и рисками ИБ.
2.4 Управление инцидентами ИБ.
2.5 Управление корректирующими и предупреждающими действиями.
2.6 Оценка эффективности СУИБ.
2.7 Внутренний аудит СУИБ.
2.8 Управление непрерывностью бизнеса.
2.9 Обучение и повышение осведомленности в области ИБ.
2.10 Вовлеченность менеджмента в вопросы информационной безопасности.
2.11 Управление соответствием регуляторным требованиям.

Для каждого требования ИБ определена форма выполнения данного требования:

- *Реализовать* – для выполнения требования необходима исключительно реализация действий, им предписанных.
- *Документировать* – для выполнения требования необходимо исключительно закрепление его положений в нормативных документах.
- *Реализовать и документировать* – для выполнения требования необходимо реализовать им предписанные действия и закрепить реализацию этих действий в нормативных документах.

Для каждого требования ИБ определены виды конфиденциальной информации в отношении которых оно применимо: коммерческая тайна, инсайдерская информация, персональные данные.

Для каждого требования ИБ определена категория, относящая его к обязательным или рекомендованным.

6.2 Перечень корпоративных требований по обеспечению информационной безопасности

6.2.1 Обеспечение информационной безопасности при работе с внешними сторонами

В отношении внешних сторон, привлекаемых для предоставления ИТ-сервисов или оказания услуг, в рамках которых они будут наделены доступом к ресурсам корпоративной сети, возникают дополнительные риски информационной безопасности, связанные с нарушением безопасности данных или работоспособности сервисов и информационных систем. В связи с этим, при подборе внешних сторон и дальнейшем взаимодействии с ними должны применяться дополнительные меры безопасности.

6.2.1.1. Должны быть заключены соглашения о неразглашении конфиденциальной информации со всеми внешними сторонами до момента предоставления им доступа к конфиденциальной информации и/или к ресурсам корпоративной сети.

6.2.1.2. Рекомендуется, при принятии решения о привлечении внешних сторон, которые могут повлиять на безопасность данных или работоспособность ИТ-сервисов, проводить формализованную оценку связанных с этими внешними сторонами рисков ИБ. Такую оценку рисков следует проводить в соответствии с установленной в Компании методикой, а результаты оценки рисков фиксировать документально.

6.2.1.3. Рекомендуется включать в отчет об оценке рисков в отношении привлекаемых внешних сторон следующую информацию:

- Наименование внешней стороны.
- Цель привлечения внешней стороны.
- Перечень ИТ-сервисов и информационных систем на безопасность и работоспособность которых может повлиять внешняя сторона.
- Виды информации (ИКТ, ИИ, ПДн) на безопасность которой может повлиять внешняя сторона.
- Результирующее значение уровня риска при привлечении внешней стороны.
- Решение, принятое в отношении внешней стороны.

6.2.1.4. Привлечение внешних сторон рекомендуется осуществлять в следующих случаях:

- Уровень, связанного с ними риска, не превышает установленный в Компании допустимый уровень риска.
- При наличии документированного решения руководства Компании о принятии риска, связанного с внешними сторонами (в случае, если допустимый уровень риска превышен).

6.2.1.5. Рекомендуется, в соответствии с регламентированными в Компании процедурами, перед использованием сервисов внешних сторон и/или предоставления им доступа к ресурсам корпоративной сети, определить применимые к этим внешним сторонам требования информационной безопасности. Все эти требования рекомендуется включать в договоры с внешними сторонами.

6.2.2 Обеспечение информационной безопасности при управлении персоналом

6.2.2.1. Должны быть регламентированы процедуры приема персонала на работу, включающие в себя следующие проверки:

- Проверку подлинности и полноты представленных при трудоустройстве сведений.
- Проверку биографических фактов кандидатов на трудоустройство.
- Проверки с целью недопущения конфликта интересов.

6.2.2.2. Должны документально фиксироваться результаты проведения кадровых проверок, а сами проверки при трудоустройстве следует проводить в соответствии с требованиями внутренних нормативных документов Компании.

6.2.2.3. Должны быть заключены со всеми работниками письменные соглашения, включающие в себя:

- Обязательство о соблюдении требований Компании в области ИБ.
- Обязательство о неразглашении сведений, составляющих коммерческую тайну Компании и персональные данные, ставшие известными сотрудникам во время работы.
- Обязательство о недопущении возникновения конфликта интересов с работодателем.
- Обязательство о приверженности корпоративным ценностям работодателя.

Такие соглашения должны заключаться непосредственно при трудоустройстве в форме, регламентированной внутренними нормативными документами Компании.

6.2.2.4. Должны применяться дисциплинарные взыскания к сотрудникам, уличенным в нарушении требований ИБ или виновным в инцидентах ИБ. Такие дисциплинарные взыскания должны применяться в соответствии с установленными процедурами, а результаты применения таких взысканий следует фиксировать документально.

6.2.2.5. Должно осуществляться своевременное лишение прав доступа увольняемых сотрудников к информационным системам и сервисам Компании. Лишение прав доступа осуществляется работниками, отвечающими за управление доступом к информационным системам, на основании уведомления от подразделения, ответственного за управление персоналом. Такое уведомление должно подаваться своевременно, до момента увольнения работника, в форме и способом, установленными внутренними нормативными документами Компании.

6.2.2.6. Должен осуществляться учет технических средств, выдаваемых работникам или закрепляемых за ними. В число таких технических средств могут входить, в том числе, рабочие станции, ноутбуки, планшеты, мобильные телефоны и съемные носители информации. При увольнении работники должны сдать эти технические средства ответственным сотрудникам Компании (заведующему складом).

6.2.3 Обеспечение информационной безопасности при работе с мобильными устройствами, используемыми для доступа к ресурсам корпоративной сети, и носителями информации

Использование мобильных устройств для доступа к ресурсам корпоративной сети увеличивает риски несанкционированного доступа и распространения конфиденциальной информации. Для снижения этих рисков, применение таких мобильных устройств должно осуществляться в строгом соответствии с установленными в Компании требованиями.

6.2.3.1. Должно быть реализовано предоставление доступа к мобильным устройствам исключительно после прохождения процедуры аутентификации. Способы аутентификации должны соответствовать принятым в Компании, в том числе, если для аутентификации применяются пароли – они должны соответствовать требованиям парольной политики Компании.

6.2.3.2. Должно применяться на планшетах и мобильных телефонах специализированное программное обеспечение, обладающее функционалом удаленного уничтожения информации.

6.2.3.3. Должны быть доведены до персонала процедуры, регламентирующие действия работников в случае утери мобильных устройств, на которых хранится или может храниться конфиденциальная информация. В число таких действий обязательно должно входить требование по извещению пользователями сотрудников Департамента по безопасности и информационным технологиям. Все случаи утери мобильных устройств должны быть обработаны в соответствии с требованиями внутренних нормативных документов, а результаты (включая уведомления от пользователей об утере) – документированы в установленной форме.

6.2.3.4. Должны применяться дополнительные меры и средства защиты для мобильных устройств, не соответствующих требованиям настоящего Стандарта и иных документов Компании в области ИБ. Недопустимо применение мобильных устройств, не соответствующих корпоративным требованиям по ИБ, для доступа к ресурсам корпоративной сети.
6.2.3.5. Должна быть установлена ответственность пользователей за физическую безопасность мобильного устройства, это требование должно быть доведено до пользователей.
6.2.3.6. Рекомендуется применять антивирусное программное обеспечение на мобильных устройствах. В случае принятия решения об использовании таких средств защиты, рекомендуется установить соответствующие требования внутренними нормативными документами Компании.
6.2.3.7. Рекомендуется применять на мобильных устройствах локальные средства межсетевого экранирования и предотвращения вторжений. В случае принятия решения об использовании таких средств защиты, рекомендуется установить соответствующие требования внутренними нормативными документами Компании.
6.2.3.8. Рекомендуется осуществлять шифрование конфиденциальной информации, хранящейся на мобильных устройствах. Рекомендуется регламентировать требования к шифрованию конфиденциальной информации на мобильных устройствах и к соответствующим средствам шифрования во внутренних нормативных документах Компании.

6.2.4 Обеспечение информационной безопасности на стадиях жизненного цикла информационных систем

Рассматриваются следующие стадии жизненного цикла информационных систем:

- Стадия разработки (проектирования) и модернизации.
- Стадия эксплуатации.
- Стадия вывода из эксплуатации.

Стадия разработки (проектирования) и модернизации:
6.2.4.1. Должно осуществляться формирование требований по ИБ к внедряемым, разрабатываемым или дорабатываемым системам. При этом требования и новый функционал должны быть согласованы с Управлением защиты информации. Результаты согласования должны быть зафиксированы документально.
6.2.4.2. Должны разрабатываться методики тестирования и проведения приемочных испытаний в каждом случае внедрения новых информационных систем, сервисов, инфраструктурных решений или доработки уже существующих. Эти методики должны включать в себя проверку выполнения ранее сформированных требований по ИБ. Приемочные испытания должны проводиться в соответствии с вышеуказанными методиками, а результаты приемочных испытаний должны быть документированы.
6.2.4.3. Должен быть назначен сотрудник, ответственный за выполнение процедуры внесения изменений в информационные системы, сервисы, настройки сетевых устройств и средств защиты информации.
6.2.4.4. Должен быть установлен перечень лиц, ответственных за согласование изменений, вносимых в информационные системы, сервисы, настройки сетевых устройств и средств защиты информации.
6.2.4.5. Должен быть реализован механизм обратимости вносимых изменений, т.е. должен существовать способ (резервная система, обратная последовательность операций, архив исходного кода системы и т.п.), позволяющий в случае необходимости вернуть изменяемый ресурс в исходное состояние.
6.2.4.6. Рекомендуется не использовать при разработке и тестировании информационных систем реальных данных продуктивных систем, содержащих конфиденциальную информацию. Рекомендуется при разработке и тестировании использовать специально подготовленные тестовые данные. Соответствующие требования, в случае их принятия, должны быть установлены внутренними нормативными документами Компании.

Стадия эксплуатации:

6.2.4.7. Должна быть реализована сегментация локальной сети Компании, как минимум в отдельные сегменты сети должны быть выделены среды разработки и тестирования. Должна осуществляться фильтрация входящего и исходящего траффика по отношению к сегментам разработки и тестирования.

6.2.4.8. Должно осуществляться внесение изменений на основании соответствующих заявок, согласованных с владельцами информационных активов, на которые могут оказать влияние планируемые к внесению изменения. Заявка на внесение изменений должна включать в себя, как минимум:

- Ожидаемое воздействие изменений на информационные ресурсы Компании.
- Описание необходимых системных, программных и человеческих ресурсов.
- Определение времени и (или) условий проведения изменений.
- Порядок действий при внесении изменений и ожидаемый результат.
- Порядок контроля результатов внесения изменений.
- Процедуры возврата к первоначальному состоянию системы.
- Критерии принятия решения об успешном завершении процесса изменения.

Аварийные (экстренные) изменения могут быть внесены без предварительного согласования на основании решения сотрудника, ответственного за выполнение процедуры внесения изменений.

6.2.4.9. Должно проводиться тестирование работоспособности информационных систем и сервисов после внесения аварийных (экстренных) изменений, в соответствии с установленными требованиями по управлению изменениями.

6.2.4.10. Должно осуществляться внесение плановых изменений исключительно после успешного завершения тестирования, если необходимость такого тестирования установлена, в соответствии с установленной процедурой управления изменениями. Результаты тестирования должны документироваться.

6.2.4.11. Должно проводиться тестирование работоспособности информационных систем и сервисов после внесения плановых изменений, не требующих предварительного тестирования. Такое тестирование проводится в соответствии с установленной процедурой управления изменениями. Результаты тестирования должны документироваться.

6.2.4.12. Рекомендуется осуществлять внесение плановых изменений на основании заранее разработанных и утвержденных планов, включающих в себя планы отката изменений. При принятии этого требования рекомендуется документировать его во внутренних нормативных документах.

6.2.4.13. Рекомендуется для всех ресурсов корпоративной сети на основании критичности обрабатываемых информационных активов и предоставляемых ими сервисов, а также с точки зрения экономической целесообразности, принять и документировать решение об очередности внесения и тестирования плановых изменений:

- Тестирование до внесения изменений (рекомендуется для большинства информационных систем).
- Тестирование после внесения изменений (допустимо для сетевого оборудования).

6.2.4.14. Рекомендуется документировать результаты внесения изменений. В случае принятия решения о документировании результатов изменений, рекомендуется регламентировать это требование во внутренних нормативных документах.

6.2.4.15. Рекомендуется перед внесением аварийных (экстренных) изменений сформировать планы откатов изменений. В случае принятия решения о формировании таких планов рекомендуется регламентировать это требование во внутренних нормативных документах.

Стадия вывода из эксплуатации:

6.2.4.16. Должно осуществляться ограничение доступа пользователей к информационным системам, переводимым в архивный режим. При этом, при наличии производственной необходимости,

пользователям может быть предоставлен доступ на чтение на основании соответствующих заявок. Перевод систем в архивный режим должен фиксировать документально актами.

6.2.4.17. Должно осуществляться уничтожение данных, содержащихся на электронных носителях (в том числе носителей резервных копий), выводимых из эксплуатации. Такое уничтожение должно проводиться с использованием методов гарантированного уничтожения.

6.2.4.18. Внутренними нормативными документами должны быть установлены требования к уничтожению бумажных носителей конфиденциальной информации. В соответствии с этими требованиями должна быть реализована процедура уничтожения бумажных носителей конфиденциальной информации надежным способом (например: в шредере, путем сжигания или при помощи специализированной компании). Такое уничтожение должно проводиться в присутствии ответственных сотрудников Компании

6.2.5 Обеспечение антивирусной защиты

6.2.5.1. Должно применяться антивирусное программное обеспечение на всех технических средствах и для всех операционных систем Компании.

6.2.5.2. Должна применяться эшелонированная антивирусная защита, предусматривающая использование средств антивирусной защиты различных производителей, в том числе на следующих компонентах корпоративной сети:

- Пользовательском оборудовании, включая на рабочие станции.
- Серверном оборудовании, включая серверы электронной почты.
- Технических средствах межсетевого экранирования.

6.2.5.3. Антивирусные средства должны обладать способностью защиты от всех известных видов вредоносного программного обеспечения. Средства антивирусной защиты должны позволять осуществлять обнаружение и нейтрализацию вредоносного ПО, содержащегося:

- На жестких дисках, съемных носителях информации и в оперативной памяти.
- В архивах и в упакованных объектах.
- В веб-траффике.
- В входящих и исходящих сообщениях электронной почты.

6.2.5.4. Антивирусное ПО должно обладать функционалом защиты от вирусов в режиме реального времени.

6.2.5.5. Должно осуществляться обновление антивирусного ПО в соответствии с заданной в Компании периодичностью, но не реже одного раза в 3 часа.

6.2.5.6. Должно выполняться антивирусное сканирование:

- Периодическое сканирование жёстких дисков и оперативной памяти с частотой, как минимум, один раз в неделю.
- При подключении съемных носителей информации.

6.2.5.7. Должны регистрироваться следующие события антивирусного ПО:

- Обнаружение вредоносного ПО и действий по результатам такого обнаружения.
- Изменение настроек антивирусного ПО.
- Обновление антивирусного ПО и вирусных сигнатур.

6.2.5.8. Должен осуществляться периодический мониторинг событий, зарегистрированных антивирусным ПО.

6.2.5.9. Рекомендуется проводить внеочередное антивирусное сканирование после внесения изменений в программную среду серверов и рабочих станций. В случае, если будет принято решение о проведении такого сканирования, соответствующее требование должно быть установлено во внутренних нормативных документах.

6.2.6 Безопасность сети и сетевого доступа

6.2.6.1. Должна поддерживаться в актуальном состоянии схема сети, для этого:

- Должен проводиться регулярный пересмотр схемы сети с целью поддержания ее актуальности.
- В схему сети должны своевременно вноситься обновления в случае любых значимых изменений в сетевой инфраструктуре.

6.2.6.2. Должны быть отражены (как минимум) на схеме сети:

- Все сегменты корпоративной сети Компании.
- Все сетевое оборудование 3-го уровня модели OSI.
- Все подключения к внешним сетям.

6.2.6.3. Должна быть реализована сегментация корпоративной сети. Сеть должна быть сегментирована в соответствии со следующими требованиями:

- Выделить в отдельный сегмент сети демилитаризованную зону (DMZ), и расположить в этом сегменте все сервисы, доступные из внешних сетей.
- Сетевые сегменты, содержащие серверы продуктивных систем, должны быть отделены от прочих сегментов ЛВС, в том числе от сегментов которые содержат рабочие станции пользователей.
- Беспроводные сети должны быть выделены в отдельные сегменты сети.

6.2.6.4. Должен быть запрещен прямой трафик из внешних сетей во внутренние сегменты корпоративной сети, за исключением сегмента DMZ.

6.2.6.5. Должна осуществляться фильтрация трафика в соответствии с требованиями внутренних нормативных документов:

- Между внешними сетями и DMZ.
- Между внутренними сегментами сети, отделенными друг от друга (в число таких сегментов входят: DMZ, серверные сегменты, сегменты пользователей, беспроводные сети).

6.2.6.6. Должны вестись реестры правил межсетевого экранирования, позволяющие осуществлять контроль правил межсетевого экранирования. Для ведения таких реестров могут использоваться специализированные автоматизированные средства. Реестры правил межсетевого экранирования должны включать в себя, как минимум все действующие правила фильтрации ЛВС.

6.2.6.7. Должен осуществляться периодический пересмотр реестра правил межсетевого экранирования для оценки актуальности правил межсетевого экранирования, а также для оценки связанных с ними рисков. Периодичность пересмотра должна быть не реже одного раза в год.

6.2.6.8. Должен быть составлен перечень разрешенных к использованию сетевых протоколов. В случае использования небезопасных протоколов (протоколов, не передающих аутентификационную информацию в зашифрованном виде), должны быть определены соответствующие защитные меры.

6.2.6.9. Должны использоваться только разрешенные к использованию протоколы, которые документированы в перечне, разработанном в соответствии с требованием предыдущего пункта.

6.2.6.10. Должен контролироваться обмен данными с внешними сетями при помощи систем обнаружения/предотвращения вторжений. Системы обнаружения/предотвращения вторжений должны контролировать весь трафик, поступающий из внешних сетей.

6.2.6.11. Должно осуществляться обновление баз данных систем обнаружения/предотвращения вторжений в соответствии с требованиями внутренних нормативных документов. Обновление сигнатур систем обнаружения/предотвращения вторжений должно осуществляться не реже одного раза в день.

6.2.6.12. Рекомендуется в реестрах правил межсетевого экранирования указывать:

- Назначение каждого правила межсетевого экранирования.
- Инициатора создания правила.

6.2.7 Регистрация и мониторинг событий информационной безопасности

6.2.7.1. Должны быть определены информационные системы и сервисы, для обеспечения безопасности и доступности которых необходимо осуществлять регулярный мониторинг событий ИБ, регистрируемых на системных компонентах, которые входят в состав этих систем и сервисов. В число

таких системных компонентов могут входить: ОС, СУБД и ППО информационных систем, а также СЗИ и сетевое оборудование.

6.2.7.2. Должен осуществляться мониторинг событий ИБ, зарегистрированных на всех системных компонентах критичных информационных систем и сервисов, а также на всех средствах защиты информации и сетевом оборудовании, в соответствии с требованиями, установленными в Компании.

6.2.7.3. Должна быть настроена регистрация событий ИБ на всех системных компонентах информационных систем, на всех средствах защиты информации и сетевом оборудовании. В число таких событий должны входить, как минимум, следующие:

- Использование механизмов идентификации и аутентификации.
- Неуспешные попытки логического доступа.
- Любые действия пользователя ИС с персональными данным (согласно пп.8 п.2 ст.19 №152-ФЗ).
- Блокировка учетной записи в результате превышения лимита неверных попыток входа.
- Любые действия, совершенные с использованием административных полномочий.
- Создание/удаление учетных записей.
- Создание/удаление групп пользователей/ролей доступа.
- Изменения настроек синхронизации системного времени.
- Запуск и остановка сервисов.
- Доступ к журналам событий ИБ.
- Срабатывание сигнатур системы обнаружения вторжений.
- Обнаружение вредоносного ПО.

6.2.7.4. Для каждого события ИБ должна регистрироваться, как минимум, следующая информация:

- Название/идентификатор системного компонента, на котором зарегистрировано событие.
- Идентификатор пользователя.
- Тип события.
- Дата и время.
- Успешным или неуспешным было событие.
- Источник события (например, ip адрес клиента, название рабочей станции и т.п.).
- Идентификатор объекта, на который повлияло событие.

6.2.7.5. Должно осуществляться хранение журналов аудита событий ИБ не менее 12 месяцев, в соответствии с установленными требованиями Компании.

6.2.7.6. Должен быть ограничен доступ к журналам аудита событий ИБ и предоставлен только тем работникам, которым он необходим для осуществления должностных обязанностей.

6.2.7.7. Должно быть синхронизировано с единым источником точного времени системное время всех информационных систем.

6.2.7.8. Должен быть реализован автоматизированный мониторинг событий ИБ при помощи специализированной системы управления событиями ИБ. При помощи системы управления событиями ИБ должно осуществляться уведомление работников Компании, ответственных за ИТ и ИБ, обо всех критичных событиях ИБ.

6.2.7.9. Должен быть определен перечень системных компонентов, подключаемых к системе управления событиями ИБ для централизованного автоматизированного мониторинга. Как минимум в число таких системных компонентов должны войти:

- Сетевое оборудование (межсетевые экраны и системы обнаружения вторжений, VPN-шлюзы и т.д.).
- Средства защиты информации.
- ОС, СУБД и ППО критичных для бизнес-процессов Компании информационных систем.

6.2.7.10. Рекомендуется осуществлять мониторинг событий ИБ в режиме 24x7. В случае принятия такого решения, следует зафиксировать режим мониторинга событий ИБ во внутренних нормативных документах Компании.

6.2.8 Управление доступом и парольная защита

С целью обеспечения предоставления доступа к информационным системам Компании только тем лицам, которым он действительно необходим, и только в том объеме, который требуется для выполнения их должностных обязанностей, должны быть регламентированы и реализованы соответствующие процедуры управления доступом.

6.2.8.1. Должны быть определены роли доступа работников для каждой информационной системы. Доступ должен предоставляться на основании ролей.

6.2.8.2. Должно осуществляться предоставление доступа к информационным системам исключительно по согласованным заявкам. При этом согласование и утверждение таких заявок должно осуществляться способом, установленным внутренними нормативными документами Компании.

6.2.8.3. Заявки на предоставление доступа должны соответствовать установленным в Компании требованиям. Как минимум, заявки на доступ должны содержать следующую информацию:

- Лицо, которому предоставляется доступ (ФИО, должность, подразделение).
- Наименование информационной системы/информационного ресурса к которому запрашивается доступ.
- Перечень запрашиваемых ролей доступа (а в случае, если роли не определены - права доступа).
- Дата предоставления доступа и обоснование предоставления доступа.
- Срок, на который предоставляется доступ.

6.2.8.4. Должен быть документирован перечень информационных ресурсов, к которым предоставляются права доступа «по умолчанию», а также сами права доступа «по умолчанию». Такие права доступа должны быть минимальными.

6.2.8.5. Должны предоставляться права доступа, которые минимально необходимы для выполнения пользователями должностных обязанностей.

6.2.8.6. Должны использоваться персонифицированные доменные и локальные учетные записи пользователей и администраторов. Запрещено использование разделяемых учетных записей.

6.2.8.7. Должны быть удалены или заблокированы локальные учетные записи, устанавливаемые производителем «по умолчанию».

6.2.8.8. Должен осуществляться учет сервисных учетных записей. Должна быть обеспечена невозможность входа пользователя в систему под сервисной учетной записью.

6.2.8.9. Должно осуществляться своевременное лишение прав доступа увольняемых сотрудников к информационным системам и сервисам Компании. Лишение прав доступа осуществляется работниками, отвечающими за управление доступом к информационным системам, на основании уведомления от подразделения, ответственного за управление персоналом. Такое уведомление должно подаваться своевременно, до момента увольнения работника, в форме и способом, установленными внутренними нормативными документами Компании.

6.2.8.10. Должна проводиться периодическая выверка (актуализация) прав доступа пользователей. Актуализация/сверка прав доступа пользователей должна проводиться с заданной периодичностью (но не реже одного раза в 6 месяцев), и должна позволять установить следующее:

- Пользователю предоставлены именно те права, которые он запрашивал.
- Заблокированы учетные записи уволенных и находящихся в длительных отпусках работников.

Все нарушения, выявленные по результатам выверки прав доступа, должны быть устранены.

6.2.8.11. Должен предоставляться доступ к информационным системам только после успешного прохождения процедуры аутентификации. В качестве аутентифицирующего фактора могут быть использованы:

- Сертификат.
- Пароль.
- Одноразовый ключ.

6.2.8.12. Должно быть обеспечено соответствие паролей следующим минимальным требованиям :

- Длина пароля должна составлять не менее 8 символов для пользовательских учетных записей и 14 символов для учетных записей администраторов.
- Пароли должны включать в себя как минимум три их четырех следующих наборов символов: - строчные буквы, заглавные буквы, цифры, специальные символы.
- Срок действия пароля должен составлять не более 60 дней для пользовательских учетных записей и 30 дней для административных учетных записей.
- Минимальный срок действия пароля должен составлять не менее 1 дня.
- Максимум, после 6 неудачных попыток ввода пароля должна осуществляться блокировка учетной записи.
- Разблокирование учетных записей должно осуществляться, как минимум, после перерыва в 30 минут или вручную администратором.
- Новый пароль пользователя должен отличаться, как минимум, от 4 предыдущих.

6.2.8.13. Должны быть настроены соответствующие парольные политики для контроля выполнения требований к паролям, регламентированным внутренними документами в области ИБ.

6.2.8.14. Должно быть обеспечено соответствие паролей сервисных учетных записей следующим требованиям:

- Длина пароля должна составлять не 14 символов.
- Пароли должны включать в себя как минимум три из четырех следующих наборов символов: - строчные буквы, заглавные буквы, цифры, специальные символы.
- Срок действия пароля должен составлять не более 6 месяцев.
- Новый пароль должен отличаться, как минимум, от 4 предыдущих.

6.2.8.15. Должно осуществляться блокирование пользовательской сессии после определенного периода неактивности. Период неактивности, после которого осуществляется блокирование пользовательского сеанса, настраивается в соответствии установленными в Компании требованиями и должен составлять не более 15 минут.

6.2.8.16. Должно выполняться хранение паролей в соответствии с установленными в Компании требованиями, в том числе:

- Не должно выполняться хранение паролей пользователями и администраторами в открытом виде. Допускается использование специализированного программного обеспечения для хранения паролей в зашифрованном виде, такое программное обеспечение должно быть одобрено Д. Кроме того пароли пользователей и администраторов могут хранится в запечатанных конвертах в сейфе, после вскрытия конвертов пароли подлежат смене.
- Хранение паролей в информационных системах должно осуществляться в виде, не позволяющем их восстановить.
- Должно осуществляться хранение паролей от сервисных учетных записей в реестре, хранящемся в сейфе Директора по инфраструктуре.

6.2.8.17. Должен быть установлен и реализован запрет передачи пользователями и администраторами средств аутентификации третьим лицам (передача паролей, сертификатов, генераторов одноразовых паролей и т.д.).

6.2.8.18. Должна быть реализована процедура восстановления паролей, включая процедуры запроса смены пароля и предоставления новых паролей пользователям, в соответствии с установленными в Компании требованиями. Восстановление паролей должно осуществляться в соответствии со следующими принципами:

- Должна проверяться принадлежность учетной записи лицу, запрашивающему смену пароля.
- Новый пароль должен быть сообщен пользователю лично.

6.2.8.19. Должна осуществляться обязательная смена пароля при первом входе в систему, если аутентификация пользователя в системе осуществляется по паролю, и пароль нового пользователя (или пароль после сброса) известен администратору.

6.2.8.20. Должны быть регламентированы требования к процедурам аутентификации при удаленном доступе. Для удаленного доступа к локальной вычислительной сети должна применяться двухфакторная аутентификация.

6.2.9 Безопасность удаленного доступа

6.2.9.1. Должно осуществляться управления удаленным доступом к ресурсам корпоративной сети в соответствии с установленными в Компании требованиями.
6.2.9.2. Должно быть реализовано предоставление удаленного доступа к ресурсам корпоративной сети по заявкам, согласованным и утвержденным в соответствии с установленной в Компании формой. Заявки на предоставление удаленного доступа должны включать в себя, в том числе:

- Лицо, которому предоставляется доступ (ФИО, должность, подразделение).
- Цель предоставления удаленного доступа.
- Наименование информационной системы/информационного ресурса к которому запрашивается удаленный доступ.
- Дата предоставления доступа и обоснование предоставления доступа.
- Срок на который предоставляется доступ.

6.2.9.3. Должно осуществляться предоставление удаленного доступа минимальному кругу лиц, которым такой доступ необходим для выполнения должностных обязанностей. В соответствии с установленными в Компании требованиями, удаленный доступ для администрирования информационных систем, средств защиты информации и сетевого оборудования должен предоставляться только выделенным работникам Компании и не должен предоставляется третьим лицам, не входящим в число работников Компании.
6.2.9.4. Должно применяться шифрование информации, передаваемой по общедоступным сетям при осуществлении удаленного доступа к ресурсам корпоративной сети Компании.
6.2.9.5. Должен быть обеспечен разрыв сессии удаленного доступа пользователя после установленного в Компании периода неактивности. Время неактивности до разрыва пользовательской сессии должно составлять не более 15 минут.
6.2.9.6. Должно быть реализовано осуществление доступа к ресурсам корпоративной сети Компании в соответствии со следующими требованиями:

- Для доступа к корпоративным ресурсам из беспроводных сетей, должна выполняться предварительная идентификация и аутентификация пользователей с использованием протокола 802.1x.
- Доступ из беспроводных сетей пользователей, не прошедших идентификацию и аутентификацию, должен предоставляться только в гостевые сегменты и/или сеть Интернет.

6.2.10 Криптографическая защита информации и управление криптографическими ключами

С целью защиты информации при хранении или при передаче по сетям связи, в Компании могут применяться средства криптографической защиты. Требования по использованию средств криптографической защиты должны быть регламентированы внутренними нормативными документами.
6.2.10.1. Должны быть документально определены стойкие алгоритмы шифрования, разрешенные для использования в Компании. В случае использования криптографических средств защиты информации, должны применяться алгоритмы шифрования, включенные в этот перечень. В Компании допускается применение следующих Российских и международных алгоритмов криптографической защиты:

- ГОСТ Р 34.10-94;
- ГОСТ Р 34.10-2001;
- ГОСТ Р 34-11-94;
- ГОСТ 28147-89;

- AES 256;
- Blowfish;
- Triple DES;
- SHA/HASH.

6.2.10.2. Должна быть определена необходимость использования средств криптографической защиты информации (включая необходимость использования сертифицированных ФСБ криптосредств) для каждого канала передачи информации, выходящего за пределы внутренней корпоративной сети Компании. Должны применяться соответствующие средства криптографической защиты информации.

6.2.10.3. В Компании должен быть установлен порядок применения сертифицированных ФСБ средств криптографической защиты информации. Выбор таких СКЗИ должен осуществляться на основании модели нарушителя безопасности информации и модели угроз.

6.2.10.4. Должно осуществляться применение сертифицированных ФСБ средств криптографической защиты информации в соответствии с лицензионными требованиями, а также в соответствии с технической документацией на СКЗИ. В том числе должна быть обеспечена реализация следующих требований:

- Должен быть ограничен доступ в помещения, где расположены сертифицированные СКЗИ и/или их компоненты.
- Должен быть выполнен контроль корректности встраивания СКЗИ, в случае, если этого требует режим эксплуатации.

6.2.10.5. Должен осуществляться учет СКЗИ, криптографических ключей и ключевых носителей информации в соответствии с установленными в Компании требованиями.

6.2.10.6. Должна осуществляться генерация криптографических ключей сотрудником, специально назначенным на эту роль.

6.2.10.7. Должен быть установлен срок действия криптографических ключей, такой срок не должен превышать 12 месяцев. По истечению срока действия или после компрометации криптографические ключи должны быть отозваны.

6.2.10.8. Должны быть регламентированы и реализованы меры по защите ключей шифрования. Такие меры включают в себя, в том числе следующие:

- Доступ к ключам шифрования должен быть ограничен минимально необходимым перечнем лиц.
- Ключи шифрования должны храниться в минимально необходимом наборе мест и форм хранения.
- Должны регистрироваться события доступа к ключам шифрования.
- Рекомендуется проводить периодический контроль целостности хранимых ключей шифрования.

6.2.10.9. Должно осуществляться хранение носителей криптографических ключей способом, исключающим возможность доступа посторонних лиц к этим ключам и/или их носителям.

6.2.11 Резервирование и резервное копирование

6.2.11.1. На основании результатов оценки рисков должен определяться перечень информационных активов, подлежащих резервному копированию, периодичность резервного копирования для каждого ресурса и срок хранения резервных копий.

6.2.11.2. Должно осуществляться при помощи специализированных систем резервное копирование информации. При этом, параметры резервного копирования, настроенные в этих системах, должны соответствовать требованиям, определенным в соответствии с пунктом 6.2.11.1.

6.2.11.3. Должен быть ограничен логический доступ к резервным копиям, а также физический доступ к их носителям.

6.2.11.4. Должно осуществляться регулярное тестирования работоспособности резервных копий, в соответствии с установленными в Компании требованиями. Такое тестирование должно проводиться по крайней мере раз в квартал. Результаты периодической проверки работоспособности резервных копий должны фиксироваться документально.

6.2.11.5. Должны осуществляться маркирование и учет носителей резервных копий в соответствии с установленными в Компании требованиями. Применяемый в Компании способ маркирования и учета носителей резервных копий должен позволять определить какие именно данные и за какие периоды содержатся на носителях резервных копий.
6.2.11.6. Рекомендуется реализовать шифрование резервных копий, при этом должно быть обеспечено выполнение требований к шифрованию, установленных разделом 6.2.10. В случае принятия решения по шифрованию резервных копий, следует регламентировать соответствующие требования во внутренних нормативных документах Компании.
6.2.11.7. Рекомендуется хранить дубликаты резервных копий в территориально удаленном хранилище для обеспечения возможности восстановления информационных систем при природных катаклизмах, стихийных бедствиях или катастрофах, результатом которых может стать недоступность хранилища резервных копий или разрушение/повреждение носителей резервных копий. В случае принятия соответствующего решения, следует регламентировать такие требования во внутренних нормативных документах Компании.

6.2.12 Управление техническими уязвимостями и безопасная конфигурация

С целью поддержания должного уровня безопасности ресурсов корпоративной сети должно осуществляться выявление уязвимостей в программном обеспечении и настройках системных компонентов информационных систем, СЗИ и сетевых устройств.
6.2.12.1. Должна отслеживаться информации об уязвимостях ресурсов корпоративной сети в соответствии с установленными в Компании требованиями. В число источников информации об уязвимостях ресурсов корпоративной сети должны входить:

- Бюллетени вендоров, новостные рассылки, а также специализированные сайты, блоги и форумы.
- Внутреннее и внешнее сканирование уязвимостей ресурсов корпоративной сети.

6.2.12.2. Должно осуществляться сканирование ресурсов корпоративной сети в соответствии с документированными в Компании требованиями и с заданной периодичностью. Периодичность сканирования должна составлять не более 1 раза в квартал. Результаты сканирования должны быть документированы.
6.2.12.3. Должна осуществляться оценка критичности выявленных уязвимостей в соответствии с регламентированными в Компании критериями.
6.2.12.4. Должна осуществляться регистрация выявленных уязвимостей, уровень которых соответствует принятому в Компании уровню критичности, начиная с которого требуется их обработка (в том числе регистрация). Должна осуществляться регистрация таких уязвимостей.
6.2.12.5. Должно осуществляться устранение выявленных уязвимостей ИБ в срок, регламентированный внутренними нормативными документами Компании, и в зависимости от их уровня критичности.
6.2.12.6. Должно осуществляться планирование сроков выполнения работ по устранению уязвимостей, фиксация результатов устранения уязвимостей, а также контроль выполнения работ по устранению уязвимостей.
6.2.12.7. Должны быть разработаны и утверждены стандарты безопасного конфигурирования для ОС, СУБД и сетевого оборудования, СЗИ и прикладного ПО. Стандарты должны включать в себя:

- Требования к идентификации/аутентификации и настройке парольной политики.
- Требования к настройкам регистрации событий ИБ.
- Требования к настройке безопасных сервисов.
- Требования к настройке производительности.
- И т.д.

Необходимость разработки стандартов конфигурирования должна быть установлена внутренними нормативными документами Компании.

6.2.12.8. Должна осуществляться настройка ОС, ППО, СУБД, СЗИ и сетевого оборудования в соответствии со стандартами безопасного конфигурирования.

6.2.13 Защита от утечек конфиденциальной информации

С целью снижения вероятности утечки конфиденциальной информации (в том числе сведений, составляющих коммерческую тайну, персональные данные и инсайдерскую информацию) в Компании должны применяться специализированные защитные средства. Требования по их применению следует установить внутренними нормативными документами Компании.
Должны применяться системы защиты от утечек данных.
6.2.13.1. Должны подлежать контролю при помощи систем предотвращения утечек данных, в соответствии с установленными в Компании требованиями:

- Порты ввода/вывода.
- Электронная почта.
- Буфер обмена.
- Передача данных с помощью веб-интерфейса.

6.2.13.2. Должно быть выполнено конфигурирование системы DLP в соответствии с требованиями, установленными внутренними нормативными документами к ее действиям при обнаружении фактов передачи конфиденциальной информации по контролируемым каналам. Как минимум, система DLP должна:

- Осуществлять регистрацию таких событий.
- Уведомлять работников подразделения информационной безопасности о срабатывании настроенных в ней правил.

6.2.13.3. Должно осуществляться реагирование работников подразделения информационной безопасности на срабатывания системы DLP, установленным в Компании образом. В частности, должна осуществляться проверка фактов передачи конфиденциальной информации, зарегистрированных DLP.

6.2.14 Защита персональных данных

Обработка и защита персональных данных в Компании должна осуществляться в соответствии с требованиями и принципами, установленными законодательством Российской Федерации. При обработке и защите ПДн необходимо выполнять требования настоящего стандарта, но не ограничиваться ими.
6.2.14.1. Должны быть разработаны внутренние нормативные документы, регламентирующие обработку и защиту ПДн. Должен быть предоставлен неограниченный доступ субъектам ПДн к документу, регламентирующему политику по обработке ПДн. При необходимости, такой документ следует опубликовать на корпоративном сайте Компании.
6.2.14.2. Должен быть регламентирован и доведен до субъектов ПДн порядок реализации прав, предоставленных им ФЗ №152 «О персональных данных».
6.2.14.3. Должны быть документированы цели обработки ПДн, а также состав и сроки обработки ПДн по отношению к каждой цели. Обработка персональных данных должна осуществляться в соответствии с документированными целями и сроками.
6.2.14.4. Должна быть определена необходимость уведомления Уполномоченного органа по защите прав субъектов ПДн о начале обработке ПДн. В случае такой необходимости соответствующее уведомление должно быть подано.
6.2.14.5. Должны быть установлены внутренними документами Компании требования к хранению ПДн, в том числе:

- Базы данных, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации должны находиться на территории РФ.
- Должен проводиться учет мест хранения ПДн.

- Должен проводиться учет носителей ПДн.

6.2.14.6. Должна осуществляться обработка ПДн только при наличии законного основания, в соответствии с установленными в Компании требования. Должны быть определены случаи, в которых необходимо получение согласия субъекта ПДн, а кроме того способ и форма получения согласия субъекта ПДн в каждом из них. Во всех таких случаях согласия на обработку ПДн должны быть получены.

6.2.14.7. Должно быть получено согласие на обработку ПДн во всех следующих случаях:

- При осуществлении трансграничной передачи ПДн на территорию стран, не обеспечивающих их адекватную защиту.
- При создании общедоступных источников ПДн (согласие субъектов ПДн на включение их данных в такие источники).
- При передаче ПДн третьим лицам.

6.2.14.8. Должно осуществляться хранение согласий на обработку ПДн в течение достаточного времени (как минимум пока обрабатываются данные субъекта ПДн).

6.2.14.9. Должен быть ограничен доступ к персональным данным в Компании, такой доступ должен предоставляться только тем сотрудникам, которым он необходим для выполнения должностных обязанностей. С этой целью в Компании должен быть разработан и утвержден перечень лиц, имеющих доступ к ПДн.

6.2.14.10. Должны быть выполнены следующие требования при поручении обработки персональных данных третьему лицу:

- Заключение соответствующего договора.
- Требования к включению в договор на поручение обработки ПДн целей их обработки.
- Договор на обработку ПДн должен устанавливать перечень ПДн и перечень допустимых действий (операций) с ПДн.
- Договор на обработку должен устанавливать требования к защите ПДн в соответствии со статьей 18.1 №152-ФЗ.

Эти требования должны быть установлены в Компании.

6.2.14.11. Должно осуществляться уведомление субъектов ПДн о начале обработки их данных в случае, если ПДн получены от третьих лиц.

6.2.14.12. Должны быть выявлены все информационные системы, обрабатывающие ПДн, а перечень таких систем должен быть документирован в соответствии с установленными в Компании требованиями.

6.2.14.13. Должны быть документированы для каждой ИСПДн:

- Перечень содержащихся в ней ПДн и субъектов, которым эти ПДн принадлежат.
- Количество субъектов, чьи ПДн содержатся в ИСПДн.
- Сроки хранения ПДн в ИСПДн.
- Перечень защитных мер, применяемых в ИСПДн для обеспечения безопасности ПДн в соответствии с требованиями законодательства РФ.

6.2.14.14. Должна быть сформирована для каждой ИСПДн Модель угроз и нарушителей ИБ в соответствии с требованиями нормативно-правовых актов РФ.

6.2.14.15. Должны быть определены и зафиксированы в соответствующих актах уровни защищенности ПДн для каждой ИСПДн с целью определения защитных мер, необходимых с точки зрения законодательства.

6.2.14.16. Должны быть определены и выполнены необходимые организационные и технические требования к защите ПДн (в соответствии с уровнями защищенности), позволяющие:

- Нейтрализовать угрозы безопасности ПДн, актуальность которых установлена Моделью угроз.
- Выполнить применимые нормы законодательства РФ в области защиты ПДн.

Соответствующие требования к средствам и мерам защиты ПДн должны быть документированы.

6.2.14.17. Должны быть включены в число мер защиты ПДн, меры по обеспечению целостности следующих системных компонентов:

- ОС и файловой системы.
- Исполняемых файлов и файлов конфигураций ППО и СЗИ.
- Виртуальных машин.

6.2.15 Защита коммерческой тайны

6.2.15.1. Должна быть обеспечена защита сведений, составляющих коммерческую тайну, в соответствии с требованиями и принципами, установленными законодательством Российской Федерации.
6.2.15.2. Должен быть введен режим коммерческой тайны. Соответствующие требования должны быть установлены внутренними нормативными документами.
6.2.15.3. Должен быть определен и утвержден перечень информации, относящейся к коммерческой тайне. Все сотрудники Компании должны быть ознакомлены с этим перечнем под роспись.
6.2.15.4. Должны быть определены требования по защите информации составляющей коммерческую тайну. Применяемые защитные меры должны обеспечивать безопасность сведений, составляющих коммерческую тайну, на всем жизненном цикле:

- При создании.
- При хранении.
- При передаче.
- При уничтожении.

6.2.15.5. Должны быть документированы и выполнены требования по установлению меток конфиденциальности на информацию, составляющую коммерческую тайну.
6.2.15.6. Должны быть определены и реализованы процедуры регистрации и учета информации составляющей коммерческую тайну.
6.2.15.7. Должна быть определена процедура изменения степени конфиденциальности информации, составляющей коммерческую тайну.

6.3 Перечень корпоративных требований по управлению информационной безопасностью

6.3.1 Документирование и управление документацией

С целью обеспечения контроля за процедурами управления информационной безопасностью, должна быть определена и документирована политика управления документацией в области информационной безопасности.
6.3.1.1. Должны быть включены в Политику управления документацией следующие требования:

- Правила разработки, согласования и утверждения документации.
- Правила внесения обновлений в документацию.
- Правила публикации обновленных документов и отмены устаревших документов.
- Правила по ведению истории изменений в документах.
- Правила по формированию номера версии документа.
- Правила маркировки документации.
- Требования к составу документов.

Вся документация, регламентирующая вопросы информационной безопасности, должна вестись в соответствии с требованиями вышеописанной политики.
6.3.1.2. Должен осуществляться периодический пересмотр нормативных документов области ИБ, как минимум в следующих случаях:

- Изменения применимых стандартов и законодательных актов в области информационной безопасности.
- Изменения внешних контрактных требований, затрагивающих вопросы информационной безопасности.
- По результатам обработки инцидентов ИБ, когда такие результаты требуют внесения изменений в меры по обеспечению информационной безопасности.
- Изменения в инфраструктуре и бизнес-процессах, затрагивающие вопросы информационной безопасности.
- По результатам оценки рисков информационной безопасности.

Должны быть закреплены в Политике управления документацией требования к пересмотру нормативных документов в области ИБ.

6.3.1.3. Должна быть обеспечена доступность актуальных версий документов, регламентирующих вопросы информационной безопасности, для всех заинтересованных лиц, которым они необходимы для выполнения должностных обязанностей. Процедуры предоставления такого доступа, а также определения перечня документов, доступных тем или иным группам лиц, должны быть документированы в Политике управления документацией.

6.3.1.4. Рекомендуется документировать и выполнять формальный порядок согласования утверждения нормативных документов в области информационной безопасности. Реализация этой рекомендации позволит обеспечить участие всех заинтересованных сторон в согласовании документов.

6.3.1.5. Рекомендуется в каждом нормативном документе определить перечень записей, порождаемых по итогам выполнения процедур, описанных в документе, и правил маркировки таких записей. Соответствующее требование по определению в документах перечня записей и требований по их маркировке рекомендуется документировать в Политике управления документацией. Реализация этой рекомендации повысит удобство использования нормативной документации в области ИБ.

6.3.2 Распределение ответственности за информационную безопасность

6.3.2.1. Должно быть обеспечено точное назначение обязанностей между работниками, задействованными в процессах обеспечения и управления информационной безопасностью. Для этого должны быть формально назначены лица и/или подразделения ответственные за:

- Обеспечение информационной безопасности в целом.
- Мониторинг событий ИБ.
- Администрирование СКЗИ.
- Мониторинг информации об уязвимостях в информационных системах.
- Устранение уязвимостей в информационных системах.
- Пересмотр документов, регламентирующих ИБ.
- Инвентаризацию активов.
- Проведение оценки рисков ИБ.
- Проведение внутренних аудитов ИБ.
- Формирование плана обработки рисков ИБ.
- Управление инцидентами ИБ (включая, реагирование, расследование, устранение и формирование корректирующих мероприятий по их итогам).
- Формирование корректирующих и предупреждающих мероприятий и контроль их реализации.
- Оценку эффективности обеспечения и управления информационной безопасностью.
- Управление непрерывностью деятельности.
- Повышение осведомленности в области ИБ.
- Отслеживание изменений в стандартах и законодательных актах в области ИБ.

- Организацию обработки ПДн.
- Организацию защиты ПДн.
- Поддержания режима коммерческой тайны.

6.3.2.2. Должен соблюдаться принцип, в соответствии с которым запрещается при проведении аудита или самоооценке проверять собственную деятельность. Кроме того, не должны совмещаться следующие роли в обязанностях одних и тех же работников:

- Пользователей ИС и администраторов ИС.
- Администраторов ИС и разработчиков ИС.
- Пользователей ИС и разработчиков ИС.
- Функции по обеспечению ИБ и контролю за выполнением такой деятельности.

6.3.3 Управление активами и рисками информационной безопасности

Для формирования списка защитных мер, адекватного существующим рискам информационной безопасности, должна проводится процедура оценки рисков информационной безопасности. Входной информацией для процедуры оценки рисков ИБ служит перечень активов, являющийся результатом процедуры управления активами.

6.3.3.1. Должна быть регламентирована процедура управления активами, отвечающая следующим требованиям:

- Включающая в себя порядок инвентаризации активов и ведения реестра активов.
- Включающая в себя шкалу для оценки ценности активов.
- Предусматривающая определение (назначение) для каждого актива владельца, при оценивающего ценность каждого актива с точки зрения свойств конфиденциальности, целостности и доступности.

6.3.3.2. Должен быть составлен реестр активов, включающей в себя:

- Наименование каждого актива, применяемого при реализации процессов обработки конфиденциальной информации.
- Описание каждого актива.
- Назначение каждого актива.
- Расположение актива.
- Указание на владельца актива.
- Ценность актива с точки зрения свойств конфиденциальности, целостности и доступности.

6.3.3.3. Должно быть выполнено утверждение реестра активов руководством Компании.

6.3.3.4. Должна проводится инвентаризация активов с периодичность не реже одного раза в год, в соответствии с установленными в Компании требованиями.

Должна быть определена и документирована методика оценки рисков информационной безопасности. Такая методика должна соответствовать следующим требованиям:

- Методика должна основываться на ценности активов, степени уязвимости активов к угрозам ИБ и вероятности реализации таких угроз.
- Предусматривать использование для оценки рисков:
    - Результатов внутренних аудитов.
    - Результаты обработки инцидентов ИБ.
    - Результатов процесса управления уязвимостями ПО.
- Методика должна быть воспроизводимой, то есть результаты двух оценок риска ИБ с использованием одних и тех же исходных данных, должны быть идентичны.
- Методика должна включать в себя методологию расчета результирующего уровня для каждого риска.
- Методика должна определять требования к составу и содержанию отчетной документации по результатам ее применения.

6.3.3.5. Должен вестись реестр угроз и уязвимостей ИБ, характерных для инфраструктуры Компании и ее бизнес процессов. Перечисленные в этом реестре угрозы и уязвимости должны использоваться рамках оценки рисков ИБ для определения уровня риска в отношении каждого актива. Реестр угроз и уязвимостей должен включать в себя перечень угроз и уязвимостей, характерных для каждого типа активов Компании.

6.3.3.6. Должны быть документированы результаты оценки рисков в Отчете об оценке рисков, включающем в себя:

- Наименование каждого актива, в отношении которого проводилась оценка рисков.
- Указание на владельца актива.
- Ценность актива с точки зрения свойств конфиденциальности, целостности и доступности.
- Угрозы и уязвимости ИБ, которым подвержен каждый актив.
- Результаты предположений о подверженности активов угрозам и уязвимостям, а также рассчитанное результирующее значение риска ИБ.

6.3.3.7. Должно быть выполнено утверждение Отчета об оценке рисков руководством Компании.

6.3.3.8. Должно быть обеспечено проведение процедуры оценки рисков ИБ с периодичностью не реже одного раза в год и для всех активов, входящих в область действия СУИБ.

6.3.3.9. Должен быть определен допустимый уровень риска информационной безопасности. Риски с результирующем уровням выше чем допустимый, должны обрабатываться в обязательном порядке. Результаты обработки таких рисков, должны быть зафиксированы в отчете, содержащем:

- Перечень рисков ИБ, уровень которых выше допустимого.
- Перечень действий по обработке каждого риска недопустимого уровня, в том числе по снижению уровня каждого такого риска.
- Перечень принятых без дополнительной обработки рисков информационной безопасности с аргументацией их принятия.

6.3.4 Управление инцидентами информационной безопасности

6.3.5.1. Должны быть определены и документированы критерии отнесения тех или иных событий ИБ к инцидентам, в число таких событий входят:

- Попытки получения несанкционированного доступа.
- События вирусного заражения.
- События, связанные с несанкционированным использованием пользовательских учетных данных.
- События утечки конфиденциальной информации.

6.3.5.2. Должна быть определена шкала критичности инцидентов, с указанием типов и/или меры критичности инцидентов, которые должны быть обработаны в обязательном порядке. В связи с этим, документированные критерии обработки инцидентов могут основываться как на уровне критичности, так и на типе инцидентов.

6.3.5.3. Должны быть определен перечень лиц, уведомляемых о каждом типе инцидентов ИБ, требующих обязательной обработки,

6.3.5.4. Должна осуществляться регистрация инцидентов ИБ, требующих обязательной обработки, с уровнем детализации, продиктованным критериями обработки инцидентов. При регистрации инцидентов ИБ должна фиксироваться следующая информация:

- Дата и время обнаружения инцидента ИБ.
- Тип инцидента ИБ.
- Краткое описание инцидента ИБ.
- Сведения о лице, сообщившем об инциденте ИБ (обнаружившем инцидент ИБ).
- Предпосылки по которым был обнаружен инцидент ИБ.
- Активы Компании, затронутые инцидентом ИБ.

- Сведения о лице, зарегистрировавшем инцидент ИБ.

6.3.5.5. Должны быть разработаны планы реагирования на инциденты ИБ, требующих обязательной обработки. Эти планы должны включать в себя:

- Последовательность действий по устранению инцидента ИБ.
- Последовательность действий по уведомлению заинтересованных лиц..
- Последовательность действий по устранению последствий инцидента ИБ.
- Временные интервалы на совершение каждого действия.
- Ответственных лиц за выполнение каждого действия в рамках реагирования на инциденты ИБ.
- Перечень лиц, уведомляемых о каждом инциденте ИБ.

Устранение инцидентов ИБ должно осуществляться в соответствии с этими планами. Планы реагирования на инциденты ИБ должны быть доведены до работников Компании, ответственных за управление инцидентами ИБ.

6.3.5.6. Должны формироваться отчеты по устранению инцидентов ИБ, требующих обязательной обработки. Эти отчеты должны включать в себя:

- Дата и время обнаружения инцидента ИБ.
- Дата и время начала инцидента ИБ.
- Тип инцидента ИБ.
- Краткое описание инцидента ИБ.
- Сведения о лице, сообщившем об инциденте ИБ (обнаружившем инцидент ИБ).
- Предпосылки по которым был обнаружен инцидент ИБ.
- Активы Компании, затронутые инцидентом ИБ.
- Сведения о лице, зарегистрировавшем инцидент ИБ.
- Действия, предпринятые для устранения инцидента ИБ.

6.3.5.7. Должно проводиться расследование причин возникновения инцидентов ИБ, требующих обязательной обработки, и последующее планирование корректирующих мероприятий, призванных не допустить возникновения подобных инцидентов в дальнейшем. Расследование инцидентов ИБ должно проводиться после завершения их устранения. Результаты расследования инцидентов ИБ должны фиксироваться в соответствующем отчете.

6.3.5.8. Рекомендуется проводить ежегодное тестирование планов реагирования на инциденты ИБ.

6.3.5 Управление корректирующими и предупреждающими действиями

6.3.6.1. Должно осуществляться планирование корректирующих и предупреждающих действий, как минимум по результатам выполнения следующих процессов ИБ:

- Оценка рисков ИБ.
- Управление инцидентами ИБ.
- Оценка эффективности СУИБ.
- Проведение внутренних и внешних аудитов ИБ.
- Реализация и тестирование планов и процедур обеспечения непрерывности деятельности и восстановления после сбоев.

Подобные планы должны содержать в себе перечень действий, направленных на совершенствованные системы информационной безопасности, сроки их реализации и ответственных за их исполнение.

6.3.6.2. Должно осуществляться утверждение Планов корректирующих и предупреждающих действий лицом, ответственным за обеспечение информационной безопасности, а выполнение таких планов должно контролироваться.

6.3.6 Оценка эффективности системы управления информационной безопасностью

С целью определения эффективности деятельности по информационной безопасности, должен быть реализован соответствующий процесс.

6.3.7.1. Должна быть документирована Методика оценки эффективности СУИБ, где для каждого процесса информационной безопасности должны быть определены критерии оценки эффективности и периодичность проведения подобной оценки.

6.3.7.2. Должен своевременно производится сбор и анализ информации (метрик эффективности), необходимой для оценки эффективности процессов ИБ, выполняемый на основе принятой в Компании Методики оценки эффективности СУИБ. В число такой информации могут входить результаты исполнения процессов ИБ, например:

- Количество зафиксированных инцидентов ИБ.
- Время, прошедшее между началом и обнаружением инцидента ИБ.
- Количество своевременно устраненных инцидентов ИБ, в результате которых злоумышленник не нанес ущерба.
- И так далее для иных процессов ИБ.

6.3.7.3. Должен формироваться отчет, содержащий результаты оценки эффективности. Отчет по результатам оценки эффективности должен включать в себя в том числе следующую информацию:

- Перечень процессов ИБ, в отношении которых проводилась оценка эффективности.
- Перечень метрик эффективности, проанализированных в отношении каждого процесса ИБ, а также их значения.
- Результирующее значение оценки эффективности каждого процесса ИБ с обоснованием такой оценки, а также прошлую оценку эффективности.
- Вывод об изменении эффективности каждого процесса ИБ, а также предпосылки, которые привели к изменению эффективности.
- Предложения по повышению эффективности процессов ИБ.

6.3.7.4. Рекомендуется в случае выявления несоответствий процессов ИБ предъявляемым к ним требованиям, формировать корректирующие действия, включаемые в соответствующий план.

6.3.7 Внутренний аудит системы управления информационной безопасностью

6.3.8.1. Должны проводится внутренние аудиты (самооценка) информационной безопасности. Внутренние аудиты должны проводится в соответствии с Программой внутренних аудитов, принимаемой на период равный одному году. Такая программа должна описывать планируемые внутренние аудиты, их области и критерии.

6.3.8.2. Должна быть определена и документирована периодичность проведения внутренних аудитов. Внутренние аудиты должны проводиться не реже одного раз в год.

6.3.8.3. Должно предшествовать проведению аудита ИБ формирование Плана аудита, описывающего сроки проведения проверок, осуществляемых в рамках проведения аудита.

6.3.8.4. Должен формироваться итоговый отчет по результатам аудита. В этот отчет должны быть включены выводы, сделанные по результатам аудита. Отчет подлежит передаче лицу, ответственному за информационную безопасность, для анализа.

6.3.8.5. Должно осуществляться разграничение ответственности за проверяемую в рамках внутреннего аудита деятельность. Лица, осуществляющие проверяемую в рамках аудита деятельность, не должны проводить ее проверку.

6.3.8 Управление непрерывностью бизнеса

6.3.9.1. Должны быть определены владельцами каждой системы следующие параметры:

- Допустимая точка восстановления (RPO) – точка во времени до начала инцидента, на момент которой должны быть восстановлены данные в информационной системе после завершения инцидента.
- Допустимое время восстановления (RTO) – точка во времени, после начала инцидента, характеризующая максимально допустимое время простоя сервиса.

Эти параметры определяет владелец информационной системы.

6.3.9.2. Должны формироваться планы обеспечения непрерывности функционирования информационных систем и планы восстановления информационных систем после сбоев, основанные на ранее определенных RPO и RTO и включающие в себя набор задокументированных процедур, которые предназначены использования в случае возникновения инцидента ведущего/приведшего к прерыванию деятельности, и направлены на обеспечение возможности продолжения выполнения Корпорацией критических важных видов деятельности на установленном приемлемом уровне.

6.3.9.3. Должны проходить периодическое тестирование разработанных планов, с периодичностью не реже одного раза в год. Результаты такого тестирования должны документально фиксироваться, а в случае выявления их неработоспособности необходимо формировать корректирующие и предупреждающие действия, включаемые в соответствующий план.

6.3.9.4. Должна осуществляться классификация событий, потребовавших применения процедур восстановления деятельности, как инцидентов информационной безопасности.

6.3.9 Обучение и повышение осведомленности в области информационной безопасности

Так как работники, даже не задействованные напрямую в обеспечении информационной безопасности, своими действиями оказывают большое влияние на информационную безопасность организации, то все сотрудники так или иначе задействованные в обработке информации ограниченного доступа или работающие с системами, содержащими такую информацию, должны на регулярной основе проходить обучение по вопросам информационной безопасности.

6.3.10.1. Должны проводиться тренинги по информационной безопасности в отношении вновь принятых работников, а также работников, изменение должностных обязанностей которых потребовало этого. В ходе таких тренингов должно проводиться ознакомление работников Компании с относящимися к ним документами, регламентирующими вопросы информационной безопасности.

6.3.10.2. Должны проводится плановые периодические (по крайней мере ежегодные) тренинги по информационной безопасности для уже работающих сотрудников. Такие тренинги, должны включать в себя применимые для их участников вопросы ИБ, обработки и защиты ПДн и информации, относящейся к коммерческой тайне. Должен проводится контроль выполнения планов обучения по ИБ.

6.3.10.3. Должны применяться заранее подготовленные и согласованные материалы для обучения по вопросам информационной безопасности.

6.3.10.4. Должна осуществляться документальная фиксация результатов обучения в области ИБ. Каждый тренинг должен заканчиваться тестированием его участников.

6.3.10.5. Должно осуществляться своевременное ознакомление работников Компании с применимыми к их должностным обязанностям новыми или актуализированными внутренними документами в области ИБ.

6.3.10 Вовлеченность менеджмента в вопросы информационной безопасности

6.3.11.1. Должны быть утверждены руководством все документы в области информационной безопасности для придания им юридической значимости. Уровень руководителя, утверждающего документ, определяется в зависимости от области действия каждого документа: все работники, на которых распространяется документ должны находиться в прямом или косвенном подчинении утверждающего лица.
6.3.11.2. Должен быть назначен куратором информационной безопасности, осуществляющим общий надзор за выполнением функций по информационной безопасности, один из руководителей лица, ответственного за обеспечения ИБ в целом.
6.3.11.3. Должен быть сформирован и выделен бюджет на информационную безопасность.
6.3.11.4. Должна быть сформирована стратегия развития информационной безопасности, утвержденная куратором ИБ. Данная стратегия должна устанавливать направление развития информационной безопасности как минимум на следующие 3 года.
6.3.11.5. Должен быть вовлечен куратор ИБ в анализ результатов выполнения следующих процессов информационной безопасности:

- Проведение внешних и внутренних аудитов ИБ.
- Оценка рисков ИБ.
- Управление инцидентами ИБ.
- Оценка эффективности процессов ИБ.

6.3.11 Управление соответствием регуляторным требованиям

6.3.12.1. Должен быть определен и документирован перечень применимых стандартов и законодательных актов в области ИБ, которым необходимо обеспечить соответствие.
6.3.12.2. Должен быть организован процесс отслеживания изменений законодательных актов и стандартов в области ИБ, в рамках которого должно осуществляться:

- Формирование мер по приведению в соответствие изменившимся требованиям.
- Планирование и реализация мероприятий по приведению в соответствие.
- Контроль и регистрация выполнения вышеописанных планов.

6.3.12.3. Должны проводится проверки соответствия применимым требованиям стандартов и законодательства в области ИБ в рамках проведения внешних или внутренних аудитов ИБ.

7 ПРОВЕРКА И ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проверка и оценка ИБ проводится в следующей форме:

- Самооценка ИБ.
- Аудит ИБ.

Самооценка ИБ проводится сотрудниками Компании самостоятельно по требованиям «Корпоративной методики проведения аудита ИБ» и «Корпоративного регламента проведения аудита ИБ».

Сбор свидетельств в рамках проведения самооценки ИБ, не является обязательным и осуществляется по решению руководителя группы проводящей самооценку ИБ.

При подготовке к аудиту ИБ рекомендуется проведение самооценки ИБ.

С целью получения независимой оценки информационной безопасности, проверка и оценка ИБ может проводится в форме аудита ИБ. Аудит ИБ проводится внешними по отношению к проверяемой Компании независимыми организациями, компетентными в проведении подобных работ (в том числе и компаниями входящими в Корпорацию), по требованиям «Корпоративной методики проведения аудита ИБ» и «Корпоративного регламента проведения аудита ИБ».

Работы по аудиту ИБ проводится по договору, фиксирующему сроки и область проведения аудита ИБ, а так же ответственность привлекаемой для аудита организации за независимость и объективность оценки.

Работы по аудиту ИБ проводятся с обязательным сбором свидетельств аудита подтверждающих сделанные в рамках аудита выводы.

Проверка и оценка ИБ должна проводится не реже одного раза в два года.

Результаты проведения проверки и оценки ИБ должны быть документально оформлены в соответствии с требованиями «Корпоративного регламента проведения аудита ИБ».