П Р И К А З

«____»_____2018 г. г. Москва №_____

Об утверждении концепции обеспечения информационной безопасности ООО «Сатурн»

В целях обеспечения раннего предупреждения угроз и усиления контроля состояния информационной безопасности в ООО «Сатурн»:

1. Утвердить Концепцию обеспечения информационной безопасности ООО «Сатурн» (Приложение № 1).
2. Руководителям структурных подразделений ООО «Сатурн» обеспечивать согласование работ в области информационных технологий и телекоммуникаций в ООО «Сатурн», а также документации, формируемой в рамках проведения указанных работ, с директором департамента по безопасности ….
3. Контроль исполнения настоящего приказа возложить на …

Генеральный директор …

Приложение №1
к приказу ООО «Сатурн»
от «__» _____ 2018 г.
№ _____

Концепция обеспечения информационной безопасности ООО «Сатурн»

2018

Оглавление

Настоящий документ представляет собой концепцию обеспечения информационной безопасности ООО «Сатурн» (далее - Компания) и определяет:

- основные принципы создания перечня критичных ресурсов, нуждающихся в защите, формируемого в процессе проведения аудита информационной безопасности и анализа рисков. Данный перечень должен включать в себя описание физических, программных и информационных ресурсов с определением степени их критичности для ООО «Сатурн»;
- основные принципы защиты, определяющие стратегию обеспечения информационной безопасности и перечень правил, которыми необходимо руководствоваться при построении системы обеспечения информационной безопасности ООО «Сатурн»;
- модель нарушителя информационной безопасности, определяемую на основе обследования ресурсов системы и способов их использования;
- модель угроз информационной безопасности и оценку рисков, связанных с их осуществлением, формируемую на основе перечня критичных ресурсов и модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба;
- требования информационной безопасности, определяемые по результатам анализа рисков;
- меры по обеспечению информационной безопасности организационного и программно-технического уровня, предпринимаемые для реализации перечисленных требований;
- ответственность работников ООО «Сатурн» за соблюдение установленных требований информационной безопасности при эксплуатации информационной системы ООО «Сатурн».

Термины и определения. Принятые сокращения

Административная сеть	ЛВС, используемая для настройки и управления активным сетевым оборудованием корпоративной сети и сетевыми средствами защиты информации.
АРМ	Автоматизированное рабочее место.
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.
БД	База данных. Представленная в объективной форме совокупность самостоятельных материалов (текста, информации), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины.
Внутренняя сеть	Внутренний участок корпоративной сети, отделенный от внешней сети (сети Интернет) и DMZ межсетевым экраном. Внутренняя сеть объединяет тестовые, административные сети и сети разработчиков.
ДБ	Департамент по безопасности Общества.

Демилитаризованная зона (DMZ)	Участок корпоративной сети, расположенный между внешним межсетевым экраном и внешним маршрутизатором, используемым для подключения корпоративной сети к сети телекоммуникационных провайдеров (сети Интернет). В DMZ размещаются серверы, используемые для взаимодействия и предоставления сетевых сервисов внешним пользователям корпоративной сети, а также серверы, которые по соображениям информационной безопасности нецелесообразно размещать во внутренней сети Общества.
ДИТ	Департамент информационных технологий.
Защищенный канал передачи данных	Логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN) либо путем их физической изоляции и размещения на контролируемой территории.
ИБ	Информационная безопасность.
Идентификация	Присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
Информационная система (ИС)	Совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью обеспечения функционирования структурных подразделений Общества. В Компании используются различные типы информационных систем для решения производственных, управленческих, учетных и иных задач.
ИС	Информационные системы.
ИТКИ	Информационно-телекоммуникационная инфраструктура.
Корпоративная сеть	Объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех подразделений Общества посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.
Критичная информация	Информация, нарушение доступности, целостности, либо конфиденциальности которой может оказать негативное влияние на функционирование

	подразделений Компании, привести к причинению Обществу материального или иного вида ущерба.
Локальная вычислительная сеть (ЛВС)	Группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.
ЛВС	Локальная вычислительная сеть. Система связи компьютеров или вычислительного оборудования (серверы, маршрутизаторы и другое оборудование). Для передачи данных могут быть использованы различные физические явления, как правило — различные виды электрических сигналов, световых сигналов или электромагнитного излучения.
Межсетевой экран (МЭ)	Программно-аппаратный комплекс, используемый для контроля доступа между различными ЛВС, входящими в состав корпоративной сети, а также для взаимодействия с внешними сетями (сетью Интернет).
Несанкционированный доступ (НСД)	Доступ к информации или действие с информацией, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.
Компания	ООО «Сатурн».
Подразделения Общества	Структурные подразделения ООО «Сатурн».
Пользователь информационной системы	Работник Общества (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в корпоративной сети Общества в установленном порядке и получившие права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.
Принцип минимизации привилегий	Один из основных руководящих принципов, используемый при назначении полномочий пользователям и администраторам сети, а также при разработке списков контроля доступа. В соответствии с этим принципом пользователям предоставляются только те полномочия и сервисы, которые являются необходимыми для выполнения ими своих служебных обязанностей.
Регистрационная (учетная) запись пользователя	Включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в

	операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п.
Сеть разработчиков	ЛВС, используемая для разработки, отладки и тестирования программного обеспечения, разрабатываемого в интересах Общества.
Сетевые (информационные) сервисы	Сетевые приложения, предоставляющие различные виды сервисов для внутренних и внешних пользователей корпоративной сети, включая DNS, FTP, HTTP, Telnet и другие.
СОИБ	Система обеспечения информационной безопасности.
Список контроля доступа (ACL)	Правила фильтрации сетевых пакетов, настраиваемые на маршрутизаторах и межсетевом экране, определяющие критерии фильтрации и действия, производимые над пакетами.
Тестовая сеть	Специальный тип ЛВС, организуемый специалистами ДИТ с целью апробации ИТ-решений перед вводом их в эксплуатацию, сравнительного тестирования программных продуктов различных производителей, новых версий программных продуктов и других тестовых целях.

1. Общие положения

СОИБ Общества представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов Общества от угроз информационной безопасности. Меры защиты организационного уровня реализуются путем проведения соответствующих мероприятий, предусмотренных ОРД Общества и внутренними документами ДБ в части информационной безопасности. Меры защиты программно-технического уровня реализуются при помощи соответствующих программно-технических средств и методов защиты информации.

Экономический эффект от внедрения СОИБ должен проявляться в виде снижения величины возможного материального, репутационного и иных видов ущерба, наносимого Обществу за счет принятия мер, направленных на формирование и поддержание режима ИБ. Эти меры призваны обеспечить:

- доступность информации - возможность за приемлемое время получить требуемую информационную услугу;
- целостность информации - актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения;
- конфиденциальность информации - защита от несанкционированного ознакомления;

- корректность - отсутствие негативных влияний средств СОИБ на работоспособность, производительность, функциональность и надежность ИС Общества.

- аутентичность информации - подтверждение подлинности и достоверности электронных документов.

Концепция ИБ Общества определяет основные принципы защиты критичных информационных ресурсов. Принципы обеспечения ИБ обуславливают необходимость применения определенных методов и технологий защиты. Определение способов реализации этих принципов путем применения конкретных программно-технических средств защиты информации и системы организационных мероприятий является предметом конкретных проектов и политик информационной безопасности, разрабатываемых на основе настоящей Концепции.

Настоящая Концепция должна пересматриваться по мере выявления новых методов и технологий осуществления атак на информационные ресурсы. Подобный пересмотр также должен производиться по мере развития ИС Общества. Рекомендуемый срок пересмотра настоящей Концепции составляет 3 (три) года (при условии отсутствия коренных изменений в структуре системы, в технологиях управления и передачи информации).

Ответственными за поддержание настоящей Концепции в актуальном состоянии и общий контроль выполнения требований по обеспечению ИБ Общества являются работники Департамента по безопасности Общества.

Ответственными за выполнение требований ИБ, определяемых настоящей Концепцией и другими организационно-распорядительными документами Компании, являются пользователи и администраторы корпоративной сети Компании, а также их руководители.

Перечень необходимых мер защиты информации определяется по результатам аудита информационной безопасности ИС Общества и анализа рисков с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения доступности информации и работоспособности программно-технических средств, обрабатывающих эту информацию.

Стратегия обеспечения ИБ должна строиться в соответствии с российским законодательством в области защиты информации, требованиями международных и технологических стандартов.

Настоящая Концепция разработана на основе нормативных и распорядительных документов в области информационной безопасности Российской Федерации.

2. Основные цели и задачи обеспечения информационной безопасности

2.1. Цели обеспечения информационной безопасности

Основными целями деятельности по обеспечению ИБ являются:

- защита интересов Общества путем предотвращения возможности нанесения ущерба или причинения иного вреда субъектам информационных

отношений в результате нарушения установленных режимов обработки информации ограниченного доступа, уничтожения, искажения и блокирования информации, используемой для принятия управленческих решений;

- повышение безопасности объектов гостиничного комплекса при применении современных информационных технологий;
- защита конституционных прав работников Общества в информационной сфере;
- организация взаимодействия с работниками Компании, в целях донесения до них требований по обеспечению информационной безопасности и повышения их осведомленности.

2.2. Задачи обеспечения информационной безопасности

Для достижения целей обеспечения ИБ Общества требуется решение следующих основных задач:

- идентификация и классификация информационных активов Общества;
- прогнозирование, выявление и оценка угроз информационной безопасности и их источников;
- создание вертикально интегрированной комплексной системы обеспечения ИБ;
- прогнозирование, выявление и оценка угроз ИБ и их источников;
- разработка и внедрение в Компании современных методов и средств обеспечения ИБ;
- организация контроля состояния и оценки эффективности системы обеспечения ИБ и реализация мер по ее совершенствованию;
- поддержание СОИБ в состоянии, устойчивом к существующим и вновь выявляемым угрозам в информационной сфере;
- повышение осведомленности работников Общества в вопросах информационной безопасности.

3. Объекты защиты

К объектам защиты Общества относятся:

- критически важная информация, образующаяся в процессе функционирования и управления гостиничным комплексом (в том числе информация, искажение которой может привести к негативным последствиям для Общества);
- информационные ресурсы, представленные в виде документированной информации на бумажных, магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, подлежащие защите в соответствии с действующим законодательством, а также модификация или утрата которых может привести к нарушению деятельности Общества;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, локальные вычислительные сети и корпоративные информационные системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение),

автоматизированные системы управления информационными и управленческими процессами, системы связи и передачи данных, технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные устройства и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для реализации процессов, обработки информации, содержащей сведения, доступ к которым ограничен в соответствии с действующим законодательством;

- технические средства и системы, не обрабатывающие информацию, но размещённые в помещениях, где обрабатывается (циркулирует) информация, содержащая сведения, доступ к которым ограничен в соответствии с действующим законодательством, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.

4. Структура информационных потоков

4.1. Внутренние информационные потоки

Внутри ИС выделяются следующие информационные потоки:

- Передача файлов между файловыми серверами и пользовательскими рабочими станциями по протоколу SMB (протокол открытого обмена информацией между АРМ пользователей и серверами на основе стека TCP/IP).
- Передача сообщений электронной почты.
- Передача юридической и справочной информации между серверами БД и пользовательскими рабочими станциями.
- Деловая переписка.
- Передача отчетной информации.
- Передача бухгалтерской информации между пользовательскими рабочими станциями и сервером БД в рамках автоматизированных систем.

4.2. Внешние информационные потоки

В качестве внешних информационных потоков используются:

- Передача финансовых и статистических отчетных документов по каналам сети передачи данных, а также с использованием съемных носителей.
- Передача платежных документов в банки.
- Обмен электронной почтой.
- Передача информации по каналам удаленного доступа.
- Различные виды информационных обменов между ИС и сетью Интернет.

4.3. Характеристика каналов взаимодействия с другими системами и точек входа

В ИС Общества используются следующие каналы взаимодействия с внешними сетями:

- Выделенный магистральный канал взаимодействия с корпоративной сетью посредством использования технологии VPN.
- Резервная линия связи с сетью Интернет.

Защита подключений к внешним сетям осуществляется при помощи межсетевых экранов и встроенных средств защиты магистрального маршрутизирующего оборудования.

Доступ к информационным ресурсам сети Интернет открыт для всех пользователей ИС посредством использования прокси-сервера с аутентификацией.

5. Основные факторы, влияющие на информационную безопасность Общества

Основными факторами, влияющими на ИБ Компании, являются:

- расширение сотрудничества Общества с партнерами;
- автоматизация бизнес-процессов;
- расширение интеграции сервисов и исполнителей при построении и развитии информационно-телекоммуникационной инфраструктуры Общества;
- рост объемов информации Компании, передаваемой по открытым каналам связи;
- рост компьютерных преступлений в мире.

6. Основные принципы обеспечения информационной безопасности

Построение архитектуры СОИБ Общества должно базироваться на соблюдении следующих основных принципов обеспечения ИБ:

- Документированная осведомленность сотрудников о правилах по обеспечению безопасности информационных ресурсов Общества.
- Осведомленность о риске информационной безопасности. Процессы обеспечения информационной безопасности затрагивают каждого сотрудника Компании, использующего его информационные активы, и накладывают на него соответствующие обязанности и ограничения.
- Персональная ответственность за нарушения требований информационной безопасности возлагается непосредственно на работников, допустивших нарушения, и руководителя подразделения, в котором нарушения допущены.
- Простота архитектуры, минимизация и упрощение связей между компонентами, унификация и упрощение компонентов, использование минимального числа протоколов сетевого взаимодействия. Система должна содержать лишь те компоненты и связи, которые необходимы для ее функционирования (с учетом требований надежности и перспективного развития).
- Апробированность решений, ориентация на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.
- Построение системы из компонентов, обладающих высокой надежностью, готовностью и обслуживаемостью.
- Управляемость, возможность сбора регистрационной информации обо всех компонентах и процессах, наличие средств раннего выявления нарушений информационной безопасности, нештатной работы аппаратуры, программ и пользователей.

- Простота эксплуатации, автоматизация максимального числа действий администраторов сети.

- Эшелонированность обороны - для каждого канала утечки информации и для каждой угрозы информационной безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

- Непрерывность защиты в пространстве и времени, невозможность обхода защитных средств - системы должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом принимаются меры по недопущению перехода систем в незащищенное состояние.

- Равная прочность обороны по всем направлениям - осуществляется регламентация и документирование всех способов доступа к ресурсам корпоративной сети. В соответствии с этим принципом запрещается создавать несанкционированные подключения к корпоративной сети и другими способами нарушать установленный порядок предоставления доступа к информационным ресурсам.

- Профилактика нарушений безопасности - в большинстве случаев для Общества экономически оправданным является принятие предупредительных мер по недопущению нарушений безопасности в отличие от мер по реагированию на инциденты, связанных с принятием рисков осуществления угроз информационной безопасности. Однако это не исключает необходимости принятия мер по реагированию на инциденты и восстановлению поврежденных информационных ресурсов. В соответствии с данным принципом должен проводиться анализ рисков, опирающийся на модель угроз информационной безопасности и модель нарушителя, определяемые настоящей Концепцией. Многие риски можно уменьшить путем принятия превентивных мер защиты.

- Минимизация привилегий - политика информационной безопасности в части предоставления прав доступа учетным записям должна строиться на основе принципа «все, что не разрешено, запрещено». Права субъектов должны быть минимально достаточными для выполнения ими своих служебных обязанностей.

- Разделение обязанностей и ответственности между администраторами корпоративной сети определяется должностными инструкциями и регламентами администрирования. В работе администраторов информационной безопасности должен соблюдаться принцип «контроль контролирующего».

- Экономическая целесообразность - обеспечение соответствия ценности информационных ресурсов Общества и величины возможного ущерба (от их разглашения, утраты, утечки, уничтожения и искажения) уровню затрат на обеспечение информационной безопасности. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать экономические показатели работы автоматизированных систем Компании, в которых эта информация циркулирует.

- Преемственность и непрерывность совершенствования. Обеспечение постоянного совершенствования мер и средств защиты информационных ресурсов и информационной инфраструктуры на основе преемственности организационных и технических решений, кадрового аппарата, анализа функционирования систем защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по ее защите, достигнутого передового отечественного и зарубежного опыта в этой области. При выборе программно-технических решений по обеспечению ИБ Общества предпочтение отдается решениям, обеспечивающим соблюдение основных принципов ИБ, а также удовлетворяющих следующим критериям:

- поддержка международных и национальных стандартов с предпочтением к отечественным стандартам;

- поддержка наибольшей степени интеграции с корпоративными программно-аппаратными платформами и используемыми средствами защиты информации;

- унификация разработчиков и поставщиков используемых продуктов;

- унификация средств и интерфейсов управления подсистемами ИБ.

7. Распределение ответственности и порядок взаимодействия

Общее руководство системой обеспечения информационной безопасности осуществляет Генеральный директор Компании, который в повседневной деятельности делегирует права на управление процессами обеспечения информационной безопасности директору по комплексной безопасности, организующего деятельность Департамента по безопасности.

Организация работ по обеспечению ИБ возлагается на директора Департамента по безопасности Общества. Методическое руководство и контроль над эффективностью предусмотренных мер защиты информации осуществляет заместитель директора департамента по информационной безопасности Департамента по безопасности, который организует следующие работы по обеспечению безопасности информационных ресурсов:

- Контроль защищенности ИТ инфраструктуры Общества от угроз ИБ осуществляется посредством:

– проведения аудита безопасности ИС;

– контроля выполнения правил утвержденных политик безопасности администраторами и пользователями корпоративной сети;

– контроля доступа к сетевым ресурсам.

- Предотвращение, выявление, реагирование и расследование нарушений ИБ посредством:

– анализа и мониторинга журналов аудита критичных компонентов корпоративной сети, включая активное сетевое оборудование, МЭ, серверы, рабочие станции и т.п.;

– мониторинга сетевого трафика с целью выявления сетевых атак;

– контроля процесса создания новых учетных записей пользователей и предоставления доступа к ресурсам корпоративной сети;

– опроса пользователей и администраторов информационных систем;

– внедрения и эксплуатации специализированных программных и программно-технических средств защиты информации;

– координации деятельности всех структурных подразделений Общества по поддержанию режима ИБ.

Наряду с ДБ в разработке и согласовании организационно-распорядительных и нормативных документов по защите информации, включая составление перечней информационных ресурсов, подлежащих защите, также участвуют следующие подразделения Общества:

- Департамент информационных технологий (ДИТ);
- Департамент управления персоналом;
- структурные подразделения Компании, в которых обрабатывается информация, требующая защиты.

Квалификационные требования, предъявляемые к работникам подразделений, отвечающих за обеспечение ИБ, содержатся в должностных инструкциях. Специалисты по информационной безопасности должны проходить регулярную переподготовку и обучение.

Согласование предоставления, изменения, отмена и контроль доступа к ресурсам корпоративной сети производятся работниками ДБ совместно с работниками ДИТ.

Работники ДИТ отвечают за осуществление настройки параметров информационной безопасности серверов и рабочих станций корпоративной сети в соответствии с техническими заданиями, разработанными ДБ, и утвержденными корпоративными документами, определяющими требуемые уровни обеспечения защиты информации для различных структурных и функциональных компонентов корпоративной сети. ДБ отвечает за разработку соответствующих спецификаций и технического задания по настройке параметров безопасности, их согласование и совместное с ДИТ тестирование работоспособности предлагаемых решений, а также за осуществление контроля их исполнения. В случае невозможности выполнения требований обеспечения информационной безопасности с помощью имеющихся технических и программных средств, работники ДИТ совместно с ДБ инициируют и реализуют соответствующие проекты по внедрению и развертыванию необходимых программно-аппаратных средств.

Обеспечение внешних подключений корпоративной сети передачи данных Общества к сети Интернет и другим внешним сетям, предоставление работникам удаленного и терминального доступа к корпоративной сети, организация VPN-каналов связи осуществляются работниками ДИТ с соблюдением требований информационной безопасности.

В случае если договоры подряда предполагают доступ подрядной организации к информационным ресурсам Компании, то такой доступ согласуется структурным подразделением Общества – куратором проекта (работ) с ДБ для согласования и определения типа доступа и перечня доступных ресурсов. По результатам согласования ДБ направляет в ДИТ заявку на подключение с указанием необходимой технической информации (тип, технология доступа, перечень пользователей, перечень ресурсов и уровень

доступа к ним и т.д.). После предоставления доступа ДБ осуществляет контроль выполнения процедур безопасности.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к конфиденциальной информации либо к ИС Компании, с этими организациями должно быть заключено соглашение о защите информации, составляющей коммерческую тайну.

8. Организация работ по защите информации

Организация и проведение работ по обеспечению ИБ Общества определяются настоящей Концепцией, действующими государственными и международными стандартами и другими нормативными и методическими документами.

Эксплуатация ИС Общества осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, с учетом требований и положений, изложенных в настоящей Концепции.

Комплекс мер по защите информации в Компании включает в себя следующие мероприятия:

- назначение ролей и распределение ответственности за использование информационных ресурсов Общества;
- разработка, реализация, внедрение и контроль исполнения планов мероприятий, политик безопасности и других документов по обеспечению ИБ;
- подготовка пользователей и технических специалистов к решению проблем, связанных с обеспечением ИБ;
- проектирование, развертывание и совершенствование программно-технической инфраструктуры СОИБ;
- аудит состояния ИБ Общества.

Техническая инфраструктура СОИБ предназначена для решения следующих задач:

- защита внешнего периметра информационно-телекоммуникационной инфраструктуры Общества от угроз со стороны внешних сетей за счет использования межсетевого экранирования, контроля удаленного доступа и мониторинга информационных взаимодействий;
- мониторинг сетевого трафика в реальном времени с целью выявления злоумышленных действий пользователей корпоративной сети и попыток осуществления НСД к ресурсам корпоративной сети со стороны внешних злоумышленников;
- защита межсетевых взаимодействий между сегментами ИС Общества;
- защита корпоративных серверов за счет использования механизмов управления доступом к серверам баз данных, файловым, информационным и почтовым серверам, регистрации и учета событий, связанных с осуществлением доступа к ресурсам корпоративных серверов, механизмов мониторинга и аудита информационной безопасности;
- комплексная антивирусная защита систем, входящих в состав корпоративной сети, за счет распределения антивирусных средств

(антивирусных сканеров, резидентных антивирусных мониторов и файловых ревизоров) по следующим уровням:

- защиты внешнего шлюза в сеть Интернет,
- защиты корпоративных серверов,
- защиты рабочих мест пользователей;

- защита прикладных подсистем, функционирующих в составе корпоративной сети, обеспечение доступности предоставляемых ими прикладных сервисов;

- защита рабочих станций за счет использования механизмов управления доступом, регистрации и учета событий, связанных с осуществлением доступа к ресурсам рабочих станций, механизмов мониторинга и аудита информационной безопасности;

- мониторинг, анализ и корреляция инцидентов информационной безопасности, происходящих в Компании.

9. Меры по обеспечению информационной безопасности

9.1. Меры по обеспечению информационной безопасности организационного уровня

СОИБ реализуется путем сочетания мер организационного и программно-технического уровней. Организационные меры состоят из мер административного уровня и процедурных мер защиты информации. Основой мер административного уровня, то есть мер, предпринимаемых руководством Компании, является политика информационной безопасности. Под политикой информационной безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика информационной безопасности определяет стратегию Общества в области ИБ, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

9.2. Меры по обеспечению информационной безопасности процедурного уровня

К процедурному уровню относятся меры безопасности, реализуемые работниками Общества. Выделяются следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

В рамках управления персоналом для каждой должности должны существовать квалификационные требования по информационной безопасности. В должностные инструкции должны входить разделы, касающиеся защиты информации. ДБ обеспечивает организацию обучения каждого работника Компании, работающего с АРМ, основным мерам обеспечения информационной

безопасности и организует отработку теоретических и практических мер такого обеспечения.

Информационная безопасность ИС Общества зависит, в том числе, и от расположения и инфраструктуры, в котором она работает. Необходимо принять меры для обеспечения физической защиты зданий и прилегающей территории, поддерживающей инфраструктуры и самих компьютеров.

При разработке проекта СОИБ предполагается адекватная реализация мер физической защиты офисных зданий и других помещений, принадлежащих или арендованных Компаниям, по следующим направлениям:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры.

Предполагается также адекватная реализация следующих направлений поддержания работоспособности:

- поддержка пользователей ИС;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Мероприятия в области информационной безопасности должны предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима информационной безопасности преследует две главные цели:

- блокирование нарушителя и уменьшение наносимого вреда;
- недопущение повторных нарушений.

Планирование восстановительных работ позволяет подготовиться к авариям ИС, уменьшить ущерб от них и сохранить способность к функционированию, хотя бы в минимальном объеме.

Механизмы контроля, существенные для Общества с юридической точки зрения, включают в себя:

- защиту персональных данных;
- охрану документов Компании, составляющих коммерческую или иную тайну;
- защиту права на интеллектуальную собственность.

9.3. Меры по обеспечению информационной безопасности программно-технического уровня

Программно-технические средства защиты располагаются на следующих рубежах:

- защита внешнего периметра ИТКИ;
- защита внутренних сетевых сервисов и информационных обменов;

- защита серверов и рабочих станций;
- защита системных ресурсов и локальных приложений на серверах и рабочих станциях;
- защита выделенного сегмента руководства Общества.

На программно-техническом уровне выполнение защитных функций ИС осуществляется следующими служебными сервисами обеспечения информационной безопасности:

- идентификация/аутентификация пользователей ИС;
- разграничение доступа объектов и субъектов информационного обмена;
- протоколирование/аудит действий легальных пользователей;
- экранирование информационных потоков и ресурсов ИТКИ;
- туннелирование информационных потоков;
- шифрование информационных потоков, критической информации;
- контроль целостности;
- контроль защищенности;
- управление СОИБ.

На внешнем рубеже информационного обмена располагаются средства выявления злоумышленной активности и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние подключения. Они вместе со средствами поддержки виртуальных частных сетей, объединяемых с межсетевыми экранами, образуют внешний периметр информационной безопасности, отделяющий информационную систему Общества от внешнего мира.

Сервис активного аудита СОИБ (как и управление) должен присутствовать во всех критически важных компонентах и, в частности, в защитных. Это позволит быстро обнаружить атаку, даже если по каким-либо причинам она окажется успешной. Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу пользователя к ИС Общества должна предшествовать идентификация и аутентификация субъектов информационного обмена (пользователей и процессов).

Средства шифрования и контроля целостности информации, передаваемой по каналам связи, целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирование.

Последний рубеж образуют средства пассивного аудита, помогающие оценить последствия реализации угроз информационной безопасности, найти виновного, выяснить, почему успех атаки стал возможным.

Расположение средств обеспечения высокой доступности определяется критичностью соответствующих сервисов или их компонентов.

10. Порядок категорирования защищаемой информации

Различаются следующие категории информационных ресурсов, подлежащих защите в Компании:

- данные, критичные для функционирования ИС и работы структурных подразделений;
- информация, составляющая коммерческую тайну;

- персональные данные работников контрагентов;
- персональные данные работников;
- персональные данные клиентов Общества;
- конфиденциальная информация (включая коммерческую тайну, служебную тайну и персональные данные), принадлежащая третьей стороне.

К первой категории данных относятся информационные ресурсы и системы Компании, нарушение целостности, доступности и конфиденциальности которых может привести к сбоям функционирования основных бизнес-процессов.

Остальные категории информации представляют собой сведения ограниченного распространения, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности информации путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Подходы к решению проблемы защиты информации в Компании, в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования бизнес-процессов Общества. Для этого выполняются следующие мероприятия:

– разрабатываются правила категорирования информации, позволяющие относить ее к различным видам конфиденциальных сведений и определять степень ее критичности для Общества;

– проводится категорирование информационных ресурсов;

– определяется порядок работы с документами, образцами, изделиями и др., содержащими конфиденциальные сведения;

– устанавливается круг лиц и порядок доступа к подобной информации;

– вырабатываются меры по контролю обращения документов, содержащих конфиденциальные сведения;

– в трудовые договоры с сотрудниками включаются обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушение порядка работы с ними и их разглашение.

Соглашение о неразглашении конфиденциальной информации подписывается всеми сотрудниками при приеме на работу.

Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Компаниям с другими организациями.

В Компании должен быть разработан и утвержден «Перечень конфиденциальных сведений». Все работники должны быть ознакомлены с этим перечнем в части, касающейся их компетенции.

11. Модель нарушителя информационной безопасности

Под нарушителем ИБ понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб информационным ресурсам Общества.

Под атакой на ресурсы корпоративной сети понимается попытка нанесения ущерба информационным ресурсам систем, подключенных к сети. Атака может осуществляться как непосредственно нарушителем, так и опосредованно, при помощи процессов, выполняющихся от лица нарушителя, либо путем внедрения в систему программных или аппаратных закладок, компьютерных вирусов, троянских программ и т.п.

В соответствии с моделью все нарушители по признаку принадлежности к подразделениям, обеспечивающим функционирование ИС, подразделяются на внешних и внутренних.

11.1. Внутренние нарушители

Внутренним нарушителем может быть лицо из следующих категорий сотрудников обслуживающих подразделений:

- обслуживающий персонал (системные администраторы, администраторы БД, администраторы приложений и т.п., отвечающие за эксплуатацию и сопровождение технических и программных средств);
- программисты, отвечающие за разработку и сопровождение системного и прикладного ПО;
- технический персонал (рабочие подсобных помещений, уборщицы и т.п.);
- работники структурных подразделений Компании, которым предоставлен доступ в помещения, где расположено компьютерное или телекоммуникационное оборудование;
- работники структурных подразделений Компании, которым предоставлен доступ к системам, входящим в состав корпоративной сети.

Предположения о квалификации внутреннего нарушителя формулируются следующим образом:

- внутренний нарушитель является высококвалифицированным специалистом в области разработки и эксплуатации ПО и технических средств;
- знает специфику задач, решаемых обслуживающими подразделениями ИС Общества;
- является системным программистом, способным модифицировать работу операционных систем;
- правильно представляет функциональные особенности работы системы и процессы, связанные с хранением, обработкой и передачей критичной информации;
- может использовать как штатное оборудование и ПО, имеющиеся в составе системы, так и специализированные средства, предназначенные для анализа и взлома компьютерных систем.

В зависимости от способа осуществления доступа к ресурсам системы и предоставляемых им полномочий внутренние нарушители подразделяются на пять категорий.

Категория А: не зарегистрированные в системе лица, имеющие санкционированный доступ в помещения с оборудованием. Лица, относящиеся к категории А могут:

- иметь доступ к любым фрагментам информации, распространяющейся по внутренним каналам связи корпоративной сети;
- располагать любыми фрагментами информации о топологии сети, об используемых коммуникационных протоколах и сетевых сервисах;
- располагать именами зарегистрированных пользователей системы и вести разведку паролей зарегистрированных пользователей.

Категория B: зарегистрированный пользователь системы, осуществляющий доступ к системе с удаленного рабочего места. Лица, относящиеся к категории B:

- располагают всеми возможностями лиц, относящихся к категории A;
- знают, по крайней мере, одно легальное имя доступа;
- обладают всеми необходимыми атрибутами, обеспечивающими доступ к системе (например, паролем);
- имеют санкционированный доступ к информации, хранящейся в БД и на файловых серверах корпоративной сети, а также на рабочих местах пользователей. Полномочия пользователей категории B по доступу к информационным ресурсам корпоративной сети Общества должны регламентироваться политикой информационной безопасности, принятой в Компании или политикой безопасности ИС, если такая политика отличается от общепринятой.

Категория C: зарегистрированный пользователь, осуществляющий локальный либо удаленный доступ к системам, входящим в состав корпоративной сети. Лица, относящиеся к категории C:

- обладают всеми возможностями лиц категории B;
- располагают информацией о топологии сети, структуре БД и файловых систем серверов;
- имеют возможность осуществления прямого физического доступа к техническим средствам ИС.

Категория D: зарегистрированный пользователь системы с полномочиями системного (сетевого) администратора. Лица, относящиеся к категории D:

- обладают всеми возможностями лиц категории C;
- обладают полной информацией о системном и прикладном программном обеспечении ИС;
- обладают полной информацией о технических средствах и конфигурации сети;
- имеют доступ ко всем техническим и программным средствам ИС и обладают правами настройки технических средств и ПО.

Концепция информационной безопасности требует подотчетности лиц, относящихся к категории D, и осуществления независимого контроля над их деятельностью.

Категория E: программисты, отвечающие за разработку и сопровождение общесистемного и прикладного ПО, используемого в ИС. Лица, относящиеся к категории E:

- обладают возможностями внесения ошибок, программных закладок, установки троянских программ и вирусов на серверах корпоративной сети;

- могут располагать любыми фрагментами информации о топологии сети и технических средствах ИС.

11.2. Внешние нарушители

К внешним нарушителям относятся лица, пребывание которых в помещениях с оборудованием без контроля со стороны работников Общества невозможно.

Внешний нарушитель:

- осуществляет перехват, анализ, модификацию и блокирование информации, передаваемой по линиям связи, проходящим вне контролируемой территории;
- осуществляет перехват и анализ электромагнитных излучений от оборудования ИС.

Предположения о квалификации внешнего нарушителя формулируются следующим образом:

- является высококвалифицированным специалистом в области использования технических средств перехвата информации;
- знает особенности системного и прикладного ПО, а также технических средств ИС;
- знает специфику задач, решаемых ИС;
- знает функциональные особенности работы системы и закономерности хранения, обработки и передачи в ней информации;
- знает сетевое и канальное оборудование, а также протоколы передачи данных, используемые в системе;
- может использовать только серийно изготовляемое специальное оборудование, предназначенное для съема информации с кабельных линий связи и из радиоканалов, а также с использованием специальных электронных устройств, возможно внедренных в импортные технические средства, входящие в информационно-телекоммуникационной инфраструктуры Общества.

При использовании модели нарушителя для анализа возможных угроз ИБ необходимо учитывать возможность сговора между внутренними и внешними нарушителями.

12. Модель угроз информационной безопасности

12.1. Защита информационных компонентов и группы угроз

В качестве объектов защиты, рассматриваемых в рамках настоящей Концепции, выступают следующие виды информационных ресурсов Общества:

- Информация (данные, телефонные переговоры и факсы), передаваемая по каналам связи.
- Информация, хранимая в базах данных, на файловых серверах и рабочих станциях, на серверах каталогов, в почтовых ящиках пользователей корпоративной сети и т.п.
- Конфигурационная информация и протоколы работы сетевых устройств, программных систем и комплексов.

Исходя из перечисленных свойств, все угрозы информационным ресурсам системы можно отнести к одной из следующих категорий:

- угрозы доступности информации, хранимой и обрабатываемой в ИС, и информации, передаваемой по каналам связи;
- угрозы целостности информации, хранимой и обрабатываемой в ИС, и информации, передаваемой по каналам связи;
- угрозы конфиденциальности информации хранимой и обрабатываемой в ИС, и информации, передаваемой по каналам связи.

Угрозы безопасности информационных ресурсов, с точки зрения реализации, можно разделить на следующие группы:

- угрозы, реализуемые с использованием технических средств;
- угрозы, реализуемые с использованием программных средств;
- угрозы, реализуемые путем использования технических каналов утечки информации.

12.2. Угрозы, реализуемые с использованием технических средств

Технические средства системы включают в себя приемо-передающее и коммутирующее оборудование, оборудование серверов и рабочих станций, а также линии связи. К данному классу относятся угрозы доступности, целостности и в некоторых случаях конфиденциальности информации, хранимой, обрабатываемой и передаваемой по каналам связи, связанные с повреждениями и отказами технических средств ИС, приемо-передающего и коммутирующего оборудования и повреждением линий связи.

Для технических средств характерны угрозы, связанные с их умышленным или неумышленным повреждением, ошибками конфигурации и выходом из строя:

- вывод из строя (умышленный или неумышленный);
- несанкционированное либо ошибочное изменение конфигурации активного сетевого оборудования и приемо-передающего оборудования;
- физическое повреждение технических средств, линий связи, сетевого и каналообразующего оборудования;
- перебои в системе электропитания;
- импульсные помехи в сети электропитания;
- отказы технических средств;
- установка непроверенных технических средств или замена вышедших из строя аппаратных компонент на неидентичные компоненты;
- хищение технических средств и долговременных носителей конфиденциальной информации вследствие отсутствия контроля над их использованием и хранением.

В качестве источников угроз безопасности для технических средств системы выступают как внешние и внутренние нарушители, так и природные явления. Среди источников угроз для технических средств можно отметить:

- стихийные бедствия;
- пожар;
- кража оборудования;
- саботаж;
- ошибки обслуживающего персонала;
- терроризм и т.п.

12.3. Угрозы, реализуемые с использованием программных средств

Это наиболее многочисленный класс угроз конфиденциальности, целостности и доступности информационных ресурсов, связанный с получением НСД к информации, хранимой и обрабатываемой в системе, а также передаваемой по каналам связи, при помощи использования возможностей, предоставляемых ПО ИС. Большинство рассматриваемых в этом классе угроз реализуется путем осуществления локальных или удаленных атак на информационные ресурсы системы внутренними и внешними злоумышленниками. Результатом успешного осуществления этих угроз становится получение НСД к информации БД и файловых систем корпоративной сети, данным, хранящимся на АРМ операторов, конфигурации маршрутизаторов и другого активного сетевого оборудования.

В этом классе рассматриваются следующие основные виды угроз:

- внедрение вирусов и других разрушающих программных воздействий;
- нарушение целостности исполняемых файлов;
- ошибки кода и конфигурации ПО, активного сетевого оборудования;
- анализ и модификация ПО;
- наличие в ПО незадекларированных возможностей, оставленных для отладки либо умышленно внедренных;
- наблюдение за работой системы путем использования программных средств анализа сетевого трафика и утилит ОС, позволяющих получать информацию о системе и о состоянии сетевых соединений;
- использование уязвимостей ПО для взлома программной защиты с целью получения НСД к информационным ресурсам или нарушения их доступности;
- выполнение одним пользователем несанкционированных действий от имени другого пользователя («маскарад»);
- раскрытие, перехват и хищение секретных кодов и паролей;
- чтение остаточной информации в оперативной памяти компьютеров и на внешних носителях;
- ошибки ввода управляющей информации с АРМ операторов в БД;
- загрузка и установка в системе нелицензионного, непроверенного системного и прикладного ПО;
- блокирование работы пользователей системы программными средствами.

Отдельно следует рассмотреть угрозы, связанные с использованием сетей передачи данных. Данный класс угроз характеризуется получением внутренним или внешним нарушителем сетевого доступа к серверам БД и файловым серверам, маршрутизаторам и активному сетевому оборудованию. Здесь выделяются следующие виды угроз, характерные для ИТКИ Общества:

- перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика;
- замена, вставка, удаление или изменение данных пользователей в информационном потоке;

- перехват информации (например, пользовательских паролей), передаваемой по каналам связи, с целью ее последующего использования для обхода средств сетевой аутентификации;

- статистический анализ сетевого трафика (например, наличие или отсутствие определенной информации, частота передачи, направление, типы данных и т.п.).

В качестве источников угроз безопасности для технических средств системы выступают как внешние, так и внутренние нарушители.

12.4. Угрозы утечки информации по техническим каналам

При проведении работ с использованием конфиденциальной информации и эксплуатации технических средств ИС возможны следующие каналы утечки или нарушения целостности информации или работоспособности технических средств:

- побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации;
- акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;
- несанкционированный доступ к информации, обрабатываемой в автоматизированных системах;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств.

Наибольшую опасность в настоящее время представляют технические средства разведки:

- акустическая разведка;
- разведка побочных электромагнитных излучений и наводок электронных средств обработки информации;
- в отдельных ситуациях могут использоваться: телевизионная, фотографическая и визуальная оптическая разведка, обеспечивающая добывание информации, содержащейся в изображениях объектов, получаемых в видимом диапазоне электромагнитных волн с использованием телевизионной аппаратуры.

Кроме перехвата информации техническими средствами разведки возможно непреднамеренное попадание конфиденциальной информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Утечка информации возможна по следующим каналам:

- радиоканалы;
- ИК-канал;
- ультразвуковой канал;
- проводные линии.

В качестве проводных линий при передаче информации к внешним средствам регистрации могут быть использованы:

- сети переменного тока;
- линии телефонной связи;
- радиотрансляционные и технологические (пожарной, охранной сигнализации, кабели телеантенн и т.п.) линии;
- специально проложенные проводные линии.

При применении лазерной аппаратуры дистанционного прослушивания, фиксирующей информативные колебания стекол в окнах помещений, возможен съем акустической информации из помещений, в которых установлены элементы системы.

В качестве источников угроз безопасности для технических средств системы выступают как внешние, так и внутренние нарушители, оснащенные специализированными средствами технической разведки.

13. Требования по обеспечению информационной безопасности

13.1. Требования к составу основных подсистем СОИБ

В состав СОИБ должны входить следующие подсистемы:

- подсистема управления политикой информационной безопасности;
- подсистема анализа и управления рисками;
- подсистема идентификации и аутентификации;
- подсистема разграничения доступа;
- подсистема оперативного мониторинга событий информационной безопасности;
- подсистема обнаружения и предотвращения вторжений;
- подсистема контроля целостности данных;
- подсистема контроля защищенности;
- подсистема сетевой безопасности и защищенного удаленного доступа;
- подсистема антивирусной защиты;
- подсистема фильтрации контента;
- подсистема защиты от утечки данных;
- подсистема управления информационной безопасностью;
- подсистема резервного копирования и восстановления информации
- подсистема предотвращения утечки информации по техническим каналам.

13.2.Требования к подсистеме управления политикой информационной безопасности

Подсистема управления политикой ИБ предназначена для поддержания в актуальном состоянии политик и других организационно-распорядительных документов по обеспечению ИБ, ознакомление всех пользователей и технического персонала ИС с содержанием этих документов, контроля осведомленности и контроля выполнения требований политики безопасности и других регламентирующих документов.

Подсистема управления политикой информационной безопасности должна:

- поддерживать, актуализировать и контролировать исполнение корпоративной политики информационной безопасности;
- обеспечивать определение единого набора правил обеспечения информационной безопасности;
- позволять создавать новые и модифицировать уже созданные политики, правила и инструкции для обеспечения информационной безопасности;
- учитывать отраслевую специфику;
- информировать работников Общества о создании и утверждении новых политик;
- фиксировать факт ознакомления работников Общества с политиками;
- проверять усвоенные знания политик;
- контролировать нарушение политик работниками Общества;
- контролировать выполнение единого набора правил защиты информации;
- информировать административный персонал о фактах нарушения политик безопасности пользователями;
- иметь средства создания отчетов.

13.3.Требования к подсистеме анализа и управления рисками

Подсистема анализа и управления рисками предназначена для сбора и анализа информации о состоянии защищенности ИС, оценки рисков, связанных с реализацией угроз ИБ, выбора комплекса контрмер (механизмов безопасности), адекватных существующим рисками и контроля их внедрения.

Подсистема анализа и управления рисками должна обеспечивать:
- автоматизацию идентификации рисков;
- возможность создания шкал и критериев, по которым можно измерять риски;
- оценку вероятностей событий;
- оценку угроз;
- анализ допустимого уровня риска;
- выбор контрмер и оценку их эффективности;
- позволять контролировать необходимый уровень обеспечения информационной безопасности (информационные риски, сбои в системах и т.п.).

13.4. Требования к подсистеме идентификации и аутентификации

Подсистема идентификации и аутентификации представляет собой комплекс программно-технических средств, обеспечивающих идентификацию пользователей ИС и подтверждение подлинности пользователей при получении доступа к информационным ресурсам. Подсистема идентификации и аутентификации включает в себя компоненты, встроенные в операционные системы, межсетевые экраны, СУБД и приложения, которые обеспечивают управление идентификационными данными пользователей, паролями и ключевой информацией, а также реализуют различные схемы подтверждения подлинности при входе пользователя в систему и получении доступа к системным ресурсам и приложениям. Встроенные средства идентификации и аутентификации дополняются наложенными средствами, обеспечивающими

строгую многофакторную аутентификацию при доступе к информационным ресурсам, синхронизацию учетных данных пользователей в различных хранилищах (например, Active Directory, Microsoft SQL, LDAP, прикладные системы и т.п.) и предоставление единой точки доступа и администрирования для всех пользователей ИС.

Наложенные средства подсистемы идентификации и аутентификации должны обеспечивать:

- поддержание идентичности и синхронизацию учетных данных в разных хранилищах (Active Directory, Microsoft SQL, LDAP, автоматизированные системы);
- комбинирование идентификационной информации из множества каталогов;
- обеспечение единого представления всей идентификационной информации для пользователей и ресурсов;
- предоставление единой точки доступа;
- безопасный вход в домен ОС Windows (Windows-десктоп и сеть) при помощи электронного идентификатора (USB-ключа или смарт-карты);
- усиленную аппаратную двухфакторную аутентификацию пользователей (электронный идентификатор и пин-код);
- строгую аутентификацию при входе в сеть Общества посредством электронного сертификата, хранимого в защищенной области памяти электронного идентификатора;
- хранение паролей к различным ресурсам (в том числе Web) и электронных сертификатов в защищенной области памяти электронного идентификатора;
- задание парольной политики;
- централизованное управление данными об используемых электронных идентификаторах (USB-ключах или смарт-картах);
- блокирование компьютера или автоматическое отключение от сети в перерывах между работой и отсоединением электронного идентификатора.

Встроенные механизмы идентификации и аутентификации должны быть реализованы на всех рубежах защиты информации в следующих объемах:

- на рубеже защиты внешнего периметра ИТКИ Общества - идентификация и аутентификация внешних пользователей сети для доступа к информационным ресурсам ЛВС на МЭ и сервере удаленного доступа;
- на рубеже сетевой инфраструктуры должна осуществляться идентификация и аутентификация пользовательских рабочих станций по именам и сетевым адресам при осуществлении доступа к сетевым сервисам ЛВС;
- на рубеже защиты серверов и рабочих станций должна осуществляться идентификация и аутентификация пользователей при осуществлении локальной или удаленной регистрации в системе;
- на рубеже прикладного ПО должна осуществляться идентификация и аутентификация пользователей указанного ПО для получения доступа к информационным ресурсам при помощи данного ПО.

Аутентификация внутренних и внешних пользователей системы осуществляется на основе следующей информации:

- на рубеже защиты внешнего периметра для аутентификации пользователей на МЭ и сервере удаленного доступа используются схемы, устойчивые к прослушиванию сети потенциальными злоумышленниками, с возможностью аппаратных носителей аутентификационной информации;

- на рубеже защиты сетевых сервисов ЛВС используются параметры клиентов сетевого уровня (IP-адреса, имена хостов) в сочетании с параметрами канального уровня (MAC-адреса) и парольными схемами аутентификации;

- на рубежах защиты серверов, рабочих станций и приложений используются парольные схемы аутентификации с использованием аппаратных носителей аутентификационной информации.

13.5. Требования к подсистеме разграничения доступа

Подсистема разграничения доступа (авторизации) использует информацию, предоставляемую сервисом аутентификации. Авторизация пользователей для доступа к информационным ресурсам ИС осуществляется на следующих уровнях программно-технической защиты:

- на уровне защиты внешнего периметра ЛВС Общества (при их подключении к внешним сетям и сети Интернет) МЭ осуществляет разграничение доступа внешних пользователей к сервисам ЛВС и внутренних пользователей к ресурсам сети Интернет и внешних сетей в соответствии с правилами, описанными в Регламенте доступа к сети Интернет;

- на уровне защиты сетевых сервисов ЛВС используются внутренние механизмы авторизации пользователей, встроенные в сетевые сервисы либо специализированные серверы авторизации;

- на уровне защиты серверов и рабочих станций ЛВС используются механизмы авторизации, встроенные в ОС, либо специализированные наложенные средства разграничения доступа;

- на уровне защиты приложений, функциональных подсистем ИС и системных ресурсов используются механизмы авторизации, встроенные в эти приложения, а также средства разграничения доступа ОС и СУБД.

Средства разграничения доступа должны исключать возможность доступа к ресурсам системы неавторизованных пользователей.

13.6. Требования к подсистеме оперативного мониторинга событий информационной безопасности

Подсистема оперативного мониторинга событий информационной безопасности предназначена для осуществления контроля за наиболее критичными компонентами сети, включающими в себя серверы приложений, баз данных и прочие сетевые серверы, межсетевые экраны, рабочие станции управления сетью, средства защиты и т.п. Компоненты этой подсистемы располагаются на всех перечисленных выше рубежах защиты (разграничения доступа) и осуществляют протоколирование, централизованный сбор и анализ событий, связанных с безопасностью (включая предоставление доступа, попытки аутентификации, изменение системных политик и пользовательских привилегий, системные сбои и т.п.). Они включают в себя как встроенные средства протоколирования и пассивного аудита, имеющиеся в составе ОС,

СУБД, приложений и т.п. и предназначенные для регистрации событий безопасности, так и наложенные средства (программные агенты), служащие для агрегирования и анализа данных аудита, полученных из различных источников. Все данные аудита поступают на выделенный сервер мониторинга, где осуществляется их хранение и обработка (фильтрация, анализ и корреляция). Просмотр и анализ этих данных осуществляется из специализированной консоли.

Подсистема выполняет следующие основные функции:

- отслеживание событий, влияющих на безопасность системы;
- регистрация событий, связанных с безопасностью, в журнале аудита;
- централизованный сбор, хранение, анализ данных журналов безопасности;
- выявление нарушений безопасности в режиме реального времени путем фильтрации, анализа и корреляции данных по событиям информационной безопасности.

Средства протоколирования и аудита должны применяться на всех рубежах защиты в следующем объеме:

- на рубеже защиты внешнего периметра должны протоколироваться как минимум следующие события:
- информация о состоянии внешнего маршрутизатора, МЭ, сервера удаленного доступа, модемов;
- действия внешних пользователей по работе с внутренними информационными ресурсами;
- действия внутренних пользователей по работе с внешними информационными ресурсами;
- попытки нарушения правил разграничения доступа на МЭ и на сервере удаленного доступа;
- действия администраторов МЭ и сервера удаленного доступа.
- на рубеже сетевой инфраструктуры должно осуществляться протоколирование информации о состоянии активного сетевого оборудования, а также структуры информационного обмена на сетевом и транспортном уровнях;
- на рубеже защиты серверов и рабочих станций средствами подсистем аудита безопасности ОС должно обеспечиваться протоколирование всех системных событий, связанных с безопасностью, включая удачные и неудачные попытки регистрации пользователей в системе, доступ к системным ресурсам, изменение политики аудита и т.п.;
- на уровне приложений должна обеспечиваться регистрация событий, связанных с их функционированием, средствами этих приложений.

Эффективность функционирования определяется следующими основными свойствами подсистемы:

- наличие средств аудита, обеспечивающих возможность выборочного контроля любых происходящих в системе событий, связанных с безопасностью;
- наличие средств централизованного управления журналами аудита, политикой аудита и централизованного анализа данных аудита по всем контролируемым системам;

- непрерывность контроля над критичными компонентами ЛВС во времени.

13.7. Требования к подсистеме обнаружения и предотвращения вторжений

Подсистема обнаружения и предотвращения вторжений предназначена для автоматического выявления нарушений безопасности критичных компонентов ИС и реагирования на них в режиме реального времени. К числу критичных компонентов ИС, с наибольшей вероятностью подверженных атакам со стороны злоумышленников, относится внешний защищенный шлюз в сеть Интернет, сервер удаленного доступа, серверная группа и рабочие станции управления сетью. Данная подсистема тесно интегрирована с подсистемой оперативного мониторинга событий информационной безопасности, т.к. она частично передает данные аудита для дальнейшего анализа и корреляции для выявления атак.

Подсистема обнаружения и предотвращения вторжений строится на традиционной для подобных систем архитектуре «агент (сенсор) - менеджер - управляющая консоль». Для сбора информации и реагирования на атаки используются сенсоры, программа-менеджер размещается на сервере аудита и отвечает за агрегирование, хранение и обработку данных аудита, управление сенсорами и автоматическую активизацию алгоритмов реагирования. Управление всей подсистемой осуществляется с консоли администратора аудита.

Сенсор подсистемы должен обнаруживать известные типы сетевых атак, включая атаки, направленные против следующих приложений:

- СУБД, Web, FTP, TELNET и почтовые серверы;
- серверы NIS, DNS, WINS, NFS и SMB;
- почтовые агенты и Web-браузеры.

Выявление сетевых и локальных атак и других нарушений безопасности, а также реагирование на них должны осуществляться в реальном времени.

13.8. Требования к подсистеме контроля целостности

Подсистема контроля целостности программных и информационных ресурсов ИС предназначена для контроля и оперативного восстановления целостности критичных файлов ОС и приложений на серверах и рабочих станциях сети, включая конфигурационные файлы, файлы данных, программы и библиотеки функций. Контроль целостности информационных ресурсов может осуществляться путем регулярного подсчета контрольных сумм файлов и их сравнения с эталонной базой данных контрольных сумм. В случае несанкционированной модификации контролируемых файлов они могут быть восстановлены с использованием средств резервного копирования и восстановления данных.

Система контроля целостности программной и информационной части ЛВС должна обеспечивать контроль неизменности атрибутов критичных файлов и их содержимого, своевременное выявление нарушений целостности критичных файлов и их оперативное восстановление. В составе системы

контроля целостности должны быть предусмотрены средства централизованного удаленного администрирования, средства просмотра отчетов по результатам проверки целостности и средства автоматического оповещения администратора информационной безопасности о выявленных нарушениях.

13.9. Требования к подсистеме контроля защищенности

Подсистема контроля защищенности предназначена для выявления и ликвидации уязвимостей отдельных подсистем СОИБ, сетевых сервисов, приложений, функциональных подсистем, системного ПО и СУБД, входящих в состав ИС. Она включает в себя средства сетевого уровня (сетевые сканеры безопасности), устанавливаемые на рабочей станции администратора информационной безопасности и предназначенные для выявления уязвимостей сетевых ресурсов путем эмуляции действий возможного злоумышленника по осуществлению удаленных атак, а также средства системного уровня, построенные на архитектуре «агент - менеджер - консоль» и предназначенные для анализа параметров конфигурации операционных систем и приложений, выявления уязвимостей, коррекции конфигурационных параметров и контроля изменения состояния операционных систем и приложений.

Сетевой сканер должен осуществлять сканирование всего диапазона TCP и UDP портов, выявлять все доступные сетевые ресурсы и сервисы, обнаруживать уязвимости различных ОС, СУБД, сетевых сервисов и приложений.

Средства анализа защищенности системного и прикладного уровней предназначены для решения следующих основных задач:

- анализ параметров конфигурации операционных систем и приложений по шаблонам с целью выявления уязвимостей, связанных с их некорректной настройкой, определения уровня защищенности контролируемых систем и соответствия политике информационной безопасности Общества;
- коррекция конфигурационных параметров операционных систем и приложений;
- контроль изменения состояния операционных систем и приложений, осуществляемый на основе мгновенных снимков их параметров и атрибутов файлов.

Средства контроля защищенности системного уровня должны выполнять проверки привилегий пользователей, политик управления паролями и регистрационных записей пользователей, параметров подсистемы резервного копирования, командных файлов, параметров системы электронной почты, настройки системных утилит и т.п.

Средства контроля защищенности системного уровня должны поддерживать распределенные конфигурации и быть интегрированы с сетевыми сканерами и со средствами сетевого управления.

13.10. Требования к подсистеме сетевой безопасности и защищенного удаленного доступа

Подсистема сетевой безопасности реализует функции сегментирования и межсетевого экранирования и защиты каналов связи. Подсистема предназначена

для разграничения межсетевого доступа на уровне сетевых протоколов и защиты ЛВС Общества от сетевых атак со стороны сети Интернет и внешних сетей, а также для защиты конфиденциальной информации, передаваемой между ЛВС различных удаленных офисов Компании, которые не связаны между собой выделенными каналами, на основе криптографических средств защиты информации.

В рамках системы должна быть сформирована и определена архитектура подключения к сетям общего пользования и создания демилитаризованной зоны (DMZ), которая может включать межсетевой экран, VPN-сервер, Web-сервер, транслятор (relay) электронной почты, вторичный кэширующий DNS-сервер, LDAP-сервер.

На рубеже сетевой инфраструктуры должны применяться средства сегментирования ЛВС. Средства сегментирования ЛВС должны строиться на технологии виртуальных ЛВС (VLAN) в соответствии с организационной структурой объединения и логикой работы подразделений Общества с информационными ресурсами.

Серверы ЛВС должны быть расположены в выделенном сегменте (сегментах). Должно быть обеспечено отсутствие рабочих мест пользователей в указанных сегментах ЛВС.

На рубеже внешнего информационного обмена должны применяться средства межсетевого экранирования. Межсетевой экран должен обеспечивать фильтрацию сетевого трафика на сетевом, транспортном и прикладном уровнях.

Средства защиты каналов связи реализуются с использованием алгоритмов криптографической защиты информации и интегрируются со средствами межсетевого экранирования.

Средства защиты каналов связи должны обеспечивать передачу данных как в зашифрованном, так и в открытом виде в зависимости от источника и получателя информации.

13.11. Требования к подсистеме защищенного удаленного доступа

Подсистема защищенного удаленного доступа применяется на рубеже внешнего информационного обмена для подключения к ЛВС мобильных пользователей.

13.12. Требования к подсистеме антивирусной защиты

Подсистема антивирусной защиты сети предназначена для решения следующих задач:

- перекрытие всех возможных каналов распространения вирусов, к числу которых относятся: электронная почта, разрешенные для взаимодействия с сетью Интернет сетевые протоколы (HTTP и FTP), съемные носители информации (CD-ROM, флэш-носители и т.п.), разделяемые папки на файловых серверах;
- непрерывный антивирусный мониторинг и периодическое антивирусное сканирование всех серверов и рабочих станций, подключаемых к ЛВС;

- автоматическое реагирование на заражение компьютерными вирусами и на вирусные эпидемии, включающее в себя: оповещения, лечение вирусов, удаление троянских программ и очистку системы, подвергнувшейся заражению;

Она строится из следующих компонентов:

- средства управления, включающие в себя управляющую консоль, серверные компоненты системы антивирусной защиты, средства протоколирования и генерации отчетов;
- средства антивирусной защиты серверов ЛВС;
- средства антивирусной защиты рабочих станций;
- средства антивирусной защиты почтовой системы (внутренних почтовых серверов и SMTP-шлюзов на внешнем периметре сети);
- антивирусный шлюз, осуществляющий антивирусный контроль HTTP и FTP трафика.

13.13. Требования к подсистеме фильтрации контента

Подсистема фильтрации контента предотвращает утечку ценной конфиденциальной информации из ИС по протоколам HTTP, FTP и SMTP, осуществляет фильтрацию спама и прочей нежелательной корреспонденции. Она реализуется на рубеже защиты внешнего периметра сети.

Подсистема фильтрации контента должна:

- предотвращать утечку ценной конфиденциальной информации из ЛВС по протоколам HTTP, FTP и SMTP путем ее блокирования и задержания до утверждения отправки;
- обеспечивать увеличение производительности труда работников путем уменьшения рекламы, рассылок и прочих, не имеющих отношения к выполняемой работе сообщений; обнаружение спама, рассылаемого и получаемого работниками Общества;
- обеспечивать помощь в выявлении неблагонадежных работников, рассылающих свои резюме и посещающих web-сервера в поисках работы;
- обеспечивать контроль электронной почты, работающей через web-интерфейсы;
- обеспечивать контроль над всей исходящей корреспонденцией путем отсеивания сообщений, имеющих непристойное содержание, для защиты репутации Общества и работников путем предотвращения случайного или намеренного распространения писем непристойного содержания с адреса Общества;
- обеспечивать русскоязычный поиск и фильтрацию почтовых сообщений;
- обеспечивать контроль использования корпоративного выхода в Интернет в личных целях;
- разграничивать доступ работников Общества к ресурсам Интернет и обеспечивать блокирование обращений к нежелательным сайтам;
- в случае необходимости осуществлять полное или частичное архивирование данных протоколов HTTP, FTP, SMTP.

13.14. Подсистема защиты от утечки данных

Подсистема защиты от утечки данных используется в целях:

- обеспечения контроля над основными каналами передачи конфиденциальной информации в электронном виде (включая локальные и сетевые способы);
- обеспечения блокирования утечек (приостановка отправки электронных сообщений или записи на USB-накопители), если эти действия противоречат принятой политике информационной безопасности;
- обеспечения обнаружения защищаемой информации по ее содержимому (независимо от формата хранения и каналов передачи);
- обеспечения контроля утечек информации в режиме немедленного реагирования и в рамках анализа архивных данных.

Подсистема должна обеспечивать следующие функциональные возможности:

- мониторинг событий случайной или преднамеренной пересылки пользователями за пределы сегментов корпоративной сети Общества конфиденциальной информации по следующим каналам:
- электронная почта (SMTP-канал);
- использование ресурсов Интернет (веб-почта, социальные сети и т.п.);
- ICQ (сообщения и файлы);
- копирование файлов на внешние устройства;
- отправка документов на печать;
- отправка сообщений и файлов посредством Skype.
- сбор и хранение всех исходящих электронных сообщений и файлов в электронном архиве с возможностью полнотекстового поиска по этому архиву, в том числе и в присоединенных к письмам файлах;
- сбор и хранение теневых копий файлов, записанных на съемные носители, отправленных на печать, в электронном архиве с возможностью полнотекстового поиска по этому архиву;
- контроль доступа к периферийным устройствам на рабочих станциях работников.

13.15. Требования к подсистеме управления информационной безопасностью (порталу информационной безопасности)

Подсистема управления информационной безопасностью предназначена для осуществления централизованного управления всеми компонентами и подсистемами СОИБ. Управление всеми компонентами СОИБ осуществляется с консоли администратора информационной безопасности, на которой устанавливаются соответствующие средства администрирования и мониторинга.

Доступ к элементам управления должен предоставляться только после обязательной процедуры аутентификации. Для аутентификации администраторов информационной безопасности должны использоваться схемы, устойчивые к прослушиванию сети потенциальным злоумышленником.

С целью обеспечения реализации принципа минимизации административных полномочий, минимизации количества ошибочных и неправомерных действий со стороны администраторов ЛВС, должен быть

определен, документирован, согласован и утвержден состав административных групп. При определении состава административных групп следует опираться на стандартный набор административных групп, имеющийся в ОС Windows.

Определение состава административных групп и выделенных им полномочий, а также порядка осуществления контроля над составом административных групп и действиями администраторов ЛВС должно быть определенно в Регламенте работы администраторов и пользователей в сети (ином ОРД, инструкции, итп.). Каждой административной группе предоставляются только те полномочия, которые необходимы для выполнения задач администрирования, определенных в Регламенте работы администраторов и пользователей в сети.

С целью упрощения задач управления доступом пользователей к ресурсам ЛВС назначение прав доступа осуществляется на уровне групп безопасности. Каждая пользовательская учетная запись входит в состав одной или нескольких групп в зависимости от принадлежности пользователя к тому или иному подразделению и его должностными обязанностями.

13.16. Подсистема резервного копирования и восстановления информации

Подсистема резервного копирования и восстановления информации должна обеспечивать:

- возможность создания резервных копий данных всех эксплуатируемых информационных систем;
- возможность резервного копирования данных всех корпоративных приложений в гетерогенной среде без их остановки;
- возможность создания иерархических резервных копий с различными показателями по скорости восстановления и стоимости хранения;
- возможность осуществления шифрования резервных копий;
- возможность создания резервной копии на быстрых носителях (дисках);
- возможность разделения и ограничения доступа к ресурсам управления для администраторов с учетом зон их ответственности;
- минимизацию объемов хранимых данных за счет использования специализированных программно-аппаратных средств дедупликации;
- минимизацию времени восстановления за счет увеличения количества поколений (циклов) резервного копирования на быстрых носителях информации;
- централизованную систему оповещений, отчетности и анализа для элементов подсистемы резервного копирования.

13.17. Требования к подсистеме предотвращения утечки информации по техническим каналам

Подсистема предотвращения утечки информации по техническим каналам предназначена для обеспечения защиты информации при ее обработке, хранении и передаче по каналам связи, а также конфиденциальной речевой информации, циркулирующей в специально предназначенных помещениях для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций,

переговоров и т.п.). Она представляет собой совокупность организационно-технических мер по физической защите помещений, каналов передачи информации и технических средств, электромагнитной развязке между информационными цепями, по которым циркулирует защищаемая информация, развязке цепей электропитания объектов защиты с помощью сетевых помехоподавляющих фильтров и других мер защиты, предпринимаемых в соответствии с требованиями и рекомендациями нормативных документов.

При проведении работ по защите конфиденциальной речевой информации, циркулирующей в защищаемых помещениях, необходимо руководствоваться соответствующими требованиями СТР-К, направленными на исключение возможности перехвата конфиденциальной речевой информации в системах звукоусиления, при осуществлении ее звукозаписи и передачи по каналам связи.

Передача конфиденциальной речевой информации по открытым проводным каналам связи, выходящим за пределы контролируемой зоны, и радиоканалам должна быть исключена. При необходимости передачи информации следует использовать защищенные линии связи. Используемые средства защиты информации должны быть сертифицированы по требованиям безопасности информации.

При защите конфиденциальной цифровой информации от утечки по техническим каналам необходимо руководствоваться следующими требованиями:

- использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;
- использование сертифицированных средств защиты информации;
- размещение объектов защиты на максимально возможном расстоянии от границы контролируемой зоны;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах контролируемой зоны;
- использование сертифицированных систем гарантированного электропитания (источников бесперебойного питания);
- развязка цепей электропитания объектов защиты с помощью сетевых помехоподавляющих фильтров, блокирующих (подавляющих) информативный сигнал;
- электромагнитная развязка между информационными цепями, по которым циркулирует защищаемая информация, и линиями связи, другими цепями вспомогательных технических средств и систем, выходящими за пределы контролируемой зоны;
- использование защищенных каналов связи;
- размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;
- организация физической защиты помещений и собственно технических средств обработки информации с использованием технических средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и носителей информации, самих средств информатизации.

14. Ответственность работников за нарушение безопасности

К работникам, нарушающим требования концепции информационной безопасности Компании, могут быть применены дисциплинарные взыскания в виде замечания, выговора или увольнения с работы.

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, работники Общества несут полную материальную ответственность в размере причиненного ущерба.

15. Механизм реализации концепции

Реализация настоящей Концепции обеспечения информационной безопасности Общества должна осуществляться на основе утвержденных конкретных программ и планов, которые ежегодно уточняются с учетом:

- федерального законодательства и нормативной базы в области защиты информации;
- международных стандартов в области информационной безопасности и IT-безопасности;
- организационно-распорядительных документов Общества;
- реальных потребностей в средствах обеспечения информационной безопасности;
- объемов финансирования, выделяемых на обеспечение информационной безопасности Общества.