ПАО «Группа Ренессанс Страхование»
www.renins.ru
info@renins.com

1115114, г. Москва, Дербеневская набережная, дом 11, этаж 10, пом. 12
Тел.: 8 495 725-10-50
Факс: 8 495 967-35-35

Приложение №1 к Приказу
№ ..... от .....

Утверждаю
Генеральный директор
Гадлиба Ю. О.

# Концепция

информационной безопасности ПАО «Группа Ренессанс Страхование»

Москва
2024

Оглавление

# 1. Термины и определения

1.1. **Компания** – ПАО «Группа Ренессанс Страхование»
1.2. **ИС** – информационные системы.
1.3. **Информационный актив** (**информация**) - данные, сведения, обрабатываемые в Компании с помощью ИС или хранящиеся на материальном носителе (электронном или бумажном).
1.4. **Владельцы информационных активов** (**информации**) - руководители подразделений Компании, в которых создаются, обрабатываются и хранятся информационные активы.
1.5. **Конфиденциальность** – обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи).
1.6. **Целостность** – обеспечение точности и полноты информации, а также методов ее обработки.
1.7. **Доступность** – обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию).
1.8. **Меры информационной безопасности** (**ИБ**) - комплекс мер по обеспечению целостности, конфиденциальности и доступности информационных активов, создаваемых, хранимых, обрабатываемых и передаваемой внутри Компании и/или за ее пределами.
1.9. **Угроза** – причина осуществления нежелательных событий, способных нанести ущерб Компании.
1.10. **Риск** – ущерб в единицу времени, который может понести Компания в случае реализации угрозы.
1.11. **Идентификация** - присвоение субъектам и/или объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
1.12. **Аутентификация** - Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.
1.13. **Безопасность информации** - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т.п.
1.14. **Несанкционированный доступ к информации (НСД)** - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.
1.15. **Защита информации** - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию воплощенная в совокупности технических и организационных мер, обеспечивающих информационную безопасность.
1.16. **Информационная система** – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи.
1.17. **Злоумышленник** - лицо, осуществляющее осознанные действия по нарушению информационной безопасности объекта защиты.
1.18. **Криптографическая защита** - защита данных при помощи криптографического преобразования данных.
1.19. **Уязвимость** - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.
1.20. **Средство защиты информации (СЗИ) - техническое, программное средство, вещество и /или материал, предназначенные или используемые для защиты информации.**
1.21. **Объект защиты информации** - информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.
1.22. **Система обеспечения информационной безопасности (СОИБ)** - совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

# 2. Общие положения

Настоящая Концепция информационной безопасности (далее – Концепция) определяет систему взглядов на проблему обеспечения безопасности информации в ПАО «Группа Ренессанс Страхование» (далее –

Компания). Концепция представляет собой систематизированное изложение целей и задач защиты, а также принципов и мер для достижения требуемого уровня безопасности информации в ИС Компании.

Концепция является методологической основой для:

- формирования и проведения единой политики информационной безопасности Компании;
- принятия управленческих решений и разработки практических действий по воплощению политики безопасности информации и комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
- координации деятельности структурных подразделений Компании, участвующих в разработке и развитии бизнес-проектов, связанных с обработкой и хранением информации, а также эксплуатации технических средств ИС;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности информации Компании.

Концепция учитывает современное состояние и ближайшие перспективы развития ИС Компании, ее цели, задачи, а также анализирует угрозы безопасности её ресурсов.
Основные положения Концепции распространяются на все структурные подразделения Компании, осуществляющие обработку и хранение информации, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования технических средств ИС.
Основные положения Концепции могут быть распространены также на подразделения других организаций и учреждений, взаимодействующие с Компанией в качестве поставщиков и потребителей (пользователей) информации

## 3. Нормативно-правовая база обеспечения информационной безопасности.

Законодательной основой настоящей Концепции являются международные и национальные правовые и нормативно-технические документы и стандарты, описывающие правоотношения в информационной сфере, содержащие требования и методические рекомендации по построению и эксплуатации информационных систем и сетей связи, а также по обеспечению информационной безопасности в них. Учитывая интеграцию Компании в международный бизнес и использование в качестве информационной среды международного сообщества сетей Интернет, международное правовое обеспечение имеет преимущественное право при обеспечении информационной безопасности Компании, если иного не предусмотрено законодательством Российской Федерации.

Нормативно-правовая база в области обеспечения информационной безопасности призвана регулировать корпоративные отношения, позволяющие обеспечить эффективное противодействие угрозам информационной безопасности. Регулирование таких отношений происходит путем наделения субъектов правоотношений правами, обязанностями и ответственностью. Регулирование правоотношений должно способствовать:

- повышению защищенности процессов обработки и хранения информации Компании.
- обеспечению безопасности интеграции корпоративной телекоммуникационной системы в глобальные информационные системы, сохранности и правомерного использования накопленных в ней информационных ресурсов.
- созданию условий для соблюдения установленных ограничений на доступ к конфиденциальной информации и сведениям, составляющим коммерческую тайну; обеспечению запрета на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия;
- созданию условий для реализации прав и свобод граждан в области духовной жизни и информационной деятельности; обеспечению конституционных прав граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Нормативно-правовую базу составляют следующие основные группы документов, которые должны учитываться при создании системы обеспечения информационной безопасности Компании:

Международное правовое обеспечение, которое составляют международные нормативные акты (Конвенции, Соглашения, Декларации) к которым присоединилась (подписала, ратифицировала) Российская Федерация, а также заключенные от лица Российской Федерации международные Договоры (Пакты). К нему относятся:

- Всеобщая декларация прав человека, утвержденная и провозглашенная Генеральной Ассамблеей ООН (1948 г.).
- Европейская Конвенция о защите прав человека и основных свобод (1996 г.).
- Директива Европейского Парламента и Совета Европейского Союза 97/66/ЕС об обработке персональных данных.
- Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR).

Международное нормативно-техническое обеспечение, которое составляют международные Стандарты, Рекомендации, Регламенты в информационной сфере и сфере информационной безопасности. К ним относятся:

- ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».
- ISO/IEC 19791 «Оценка безопасности АС».
- ISO/IEC 17799:2000 «Управление ИБ».
- ISO27001 (ISO/IEC 27001:2005) Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью.
- ISO27002 (ISO/IEC 27002:2005) Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.
- ISO27003 Руководство по внедрению системы управления информационной безопасностью.
- ISO27004 Измерение эффективности системы управления информационной безопасностью.
- ISO27005 (BS 7799-3:2006) Управление рисками информационной безопасности.
- ISO27006 ISO/IEC 27006:2007 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью.

Национальное правовое обеспечение, которое составляют нормативные акты Российской Федерации, подзаконные акты, а также нормативные и подзаконные акты субъектов Российской Федерации. К ним относятся:

- Конституция Российской Федерации.
- Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»

Национальное нормативно-техническое обеспечение, которое составляют действующие в Российской Федерации технические регламенты, стандарты (государственные, отраслевые), руководящие документы, а также подзаконные акты уполномоченных федеральных органов государственной власти в основном нормативно-технического характера. К ним относятся руководящие документы ФСБ, ФСТЭК, РСА, Центрального Банка.

## 4. Цели и задачи обеспечения безопасности информации

Главной целью обеспечения информационной безопасности Компании является обеспечение нормальной производственной деятельности структурных подразделений Компании, основанной на обработке информации различного вида, защите законных интересов Компании от противоправных посягательств, предотвращение (минимизация) материального и морального ущерба, связанного с разглашением, искажением и/или уничтожением служебной информации. Указанная цель достигается посредством обеспечения и постоянного поддержания основных свойств информации и автоматизированной системы ее обработки - конфиденциальности, целостности и доступности.

Для достижения этого система безопасности Компании должна обеспечивать эффективное решение следующих задач:

- формирование единой политики Компании в области обеспечения безопасности ИС при ее создании, развитии и эксплуатации;
- координация деятельности всех структурных подразделений Компании и внешних организаций в вопросах, касающихся обеспечения безопасности информационных активов;
- совершенствование и стандартизация применяемых методов и средств защиты информации;
- выявление и прогнозирование внутренних и внешних угроз информационной безопасности, разработка и осуществление комплекса адекватных и экономически обоснованных мер по их предупреждению и нейтрализации;
- адаптация системы обеспечения информационной безопасности Компании к изменениям условий и среды функционирования инфраструктуры Компании, а также её структуры;
- повышение и поддержание на достаточном уровне осведомлённости работников компании в вопросах информационной безопасности.

Для устранения или сведения к минимуму возможного ущерба от действий потенциальных нарушителей информационной безопасности в Компании должны предприниматься упреждающие меры предотвращения нарушений ИБ, включая активный поиск актуальных угроз и уязвимостей с целью превентивного принятия мер, направленных на снижение уровня риска информационной безопасности до начала фактической реализации угроз.

Такие меры обеспечиваются созданием, поддержанием и развитием системы обеспечения информационной безопасности, включающей организационные, организационно-технические и технические меры защиты информации

## 5. Объекты защиты

ИС Компании предназначена для комплексного решения задач информатизации и автоматизации страхового бизнеса и обеспечения корпоративного документооборота.

ИС Компании представляет собой совокупность информационных активов, коммуникационных и вычислительных средств, общесистемного и прикладного программного обеспечения. Основой для организации взаимодействия прикладных информационных систем и индивидуальных пользователей, реализующую функции по обеспечению обработки, передачи и хранения информации Компании служит ИТ инфраструктура. Основными задачами ИС являются:

- обеспечение информационного взаимодействия между структурными подразделениями Компании или внешних организаций и субъектов с Компанией;
- организация и поддержание системы документооборота Компании;
- автоматизация бизнес-процессов Компании в целом;
- автоматизация деятельности должностных лиц (сотрудников) Компании;
- предоставления унифицированного доступа пользователей Компании и внешних клиентов к информационным ресурсам;
- обеспечение комплексной защиты циркулирующей информации на всех этапах ее обработки, хранения и передачи.

В Компании циркулирует информация разных категорий. Защищаемая информация может быть совместно использована различными пользователями из различных подсетей единой вычислительной сети.

Некоторые подразделения Компании взаимодействуют с внешними (государственными и коммерческими, российскими и зарубежными) организациями по выделенным каналам и сетям передачи данных общего пользования.

ИС Компании, как объект информационной защиты имеет следующие основные особенности:

- большое количество субъектов с различными полномочиями по доступу к данным, ресурсам и сервисам ИС;
- большое разнообразие решаемых задач, типов обрабатываемых сведений (данных), способов представления информации;
- объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;
- наличие большого числа каналов взаимодействия с внешним миром (источниками и потребителями информации);

- территориальная распределенность инфраструктуры и ее неоднородность, наличие удаленных, управляемых дистанционно объектов;
- необходимость непрерывности функционирования ИС Компании;
- значительная зависимость бизнес-процессов Компании от функционирования ИС.

Объекты информатизации ИС Компании включают:

- информационные активы, содержащие сведения ограниченного доступа и представленные в виде документов или записей в носителях на магнитной, оптической и другой основе, информационных массивах и базах данных;
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение);
- технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);
- автоматизированные системы связи и передачи данных (средства телекоммуникации и каналы связи);
- служебные помещения, в которых производятся процессы обработки информации и размещается технологическое оборудование.

Основными объектами защиты в Компании являются информационные активы, представленные в виде документов и массивов информации, независимо от формы и вида их представления:

- составляющие коммерческую тайну, доступ к которым ограничен собственником информации (Компанией);
- сведения о частной жизни граждан и иная информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (персональные данные), доступ к которым ограничен в соответствии с законодательством РФ;
- процессы обработки информации в АС – информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический персонал разработчиков и пользователей системы и ее обслуживающий персонал;
- информационная инфраструктура, включающая системы обработки, передачи, отображения и хранения информации, объекты и помещения, в которых размещены чувствительные компоненты АС.
- программно-технические средства защиты информации.

Особенности построения и функционирования ИС Компании обусловливают наличие реальных угроз и потенциальных нарушителей информационной безопасности. СОИБ Компании должна строиться в соответствии с результатами анализа угроз, обусловленных наличием потенциального нарушителя, и уязвимостей объектов защиты, на которые эти угрозы распространяются

# 6. Основные угрозы безопасности информации ИС Компании

## 6.1. Классификация угроз ИБ

Под угрозой информационной безопасности понимается возможность нарушения одной из качественных характеристик информации – конфиденциальности, целостности и доступности, вследствие воздействия нарушителя.

По виду причиняемого ущерба угрозы ИБ подразделяются на:

- угрозы нарушения конфиденциальности информации, реализация которых может привести к разглашению сведений, составляющих коммерческую тайну, а также персональных данных.
- угрозы нарушения доступности информационных ресурсов, реализация которых может привести к блокированию доступа к информации, срыву своевременного решения бизнес задач, падению качества предоставляемых услуг и сервисов, нарушению технологических процессов.
- угрозы нарушения целостности и достоверности информации, реализация которых может привести к искажению и/или разрушению информации в подсистемах сети. Кроме того, реализация данного класса угроз способна нарушить функционирование прикладного ПО и предоставить потенциальному злоумышленнику плацдарм для развития атаки на систему.

По признаку отношения к природе возникновения угрозы делятся на объективные и субъективные, а по отношению к объекту информатизации - на внутренние и внешние.

Объективные внутренние угрозы характеризуются воздействием на информацию во время ее обработки штатными средствами (передача по каналам связи, ПЭМИ, и т.д.).

Объективные внешние угрозы представляют собой техногенные явления, природные явления и стихийные бедствия.

Субъективные внешние и внутренние угрозы связаны с деятельностью человека – нарушителя.

6.2. Источники угроз ИБ

Основными источниками субъективных угроз безопасности информации Компании являются:

- непреднамеренные (ошибочные, случайные, небрежные, без злого умысла и корыстных целей) действия сотрудников Компании, связанные с нарушениями установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации при эксплуатации ИС, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности отдельных ПК, подсистем или ИС в целом;
- преднамеренные (в корыстных целях, по принуждению третьими лицами, по легкомыслию, необоснованной самоуверенности, со злым умыслом и т.п.) действия сотрудников подразделений Компании, допущенных к работе с информационными активами Компании, по реализации угроз информационной безопасности;
- противоправная деятельность криминальных структур, недобросовестных конкурентов, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности системы в целом и ее отдельных компонент;
- воздействия из внешних, по отношению к ИС Компании, информационных сетей (прежде всего Интернет) через легальные или несанкционированные каналы подключения сети Компании к таким сетям. С использованием недостатков (уязвимостей) протоколов обмена, аппаратных средств, программного обеспечения и СЗИ;
- Ошибки, допущенные при разработке бизнес-проектов или процессов, и средств защиты. Ошибки в программном обеспечении, отказы и сбои технических средств ИС Компании.

6.3. Пути реализации непреднамеренных субъективных внутренних угроз безопасности информации в ИС Компании:

- Неумышленная порча оборудования, удаление, искажение программ, файлов с важной информацией, повреждение каналов связи, порча носителей информации, приводящие к потере данных, частичному или полному отказу сервисов или нарушению работоспособности аппаратных или программных средств; изменению режимов работы устройств и программ.
- Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности информационных служб или сервисов (зависания или зацикливания) или произвести безвозвратное уничтожение данных.
- Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием информационных и вычислительных ресурсов.
- Непреднамеренное заражение ПК вредоносным ПО.
- Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования или ЭЦП, идентификационных карточек, пропусков и т.п.).
- Утеря носителей информации или копий документов.
- Утрата технических средств обработки информации, содержащих сведения, составляющие коммерческую тайну, или активные (сохранённые) сеансы связи с корпоративными ИС.
- Игнорирование организационных ограничений (установленных правил) при работе с информацией.
- Некомпетентное использование, настройка или неправомерное отключение средств защиты информации.
- Ввод ошибочных данных.

6.4. Пути реализации преднамеренных субъективных (внутренних и внешних) угроз безопасности информации в ИС Компании

- Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов автоматизированной системы (устройств, носителей важной системной информации и т.п.),

отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, линий связи и т.п.).

- Совершение в отношении сотрудников Компании противоправных действий, влекущих нарушение бизнес-процессов, выполняемых с участием таких сотрудников, а также принуждение сотрудников Компании (путем подкупа, шантажа, угроз и т.п.), имеющих определенные полномочия по доступу к защищаемым информационным активам, к совершению действий, наносящих ущерб информационной безопасности Компании.
- Хищение носителей информации, содержащих конфиденциальную информацию.
- Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.
- Незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы программными закладками и т.д.) с последующей маскировкой под зарегистрированного пользователя.
- Несанкционированное использование ПК пользователей, имеющих уникальные физические характеристики.
- Несанкционированная модификация программного обеспечения – внедрение вредоносного ПО.
- Перехват и анализ потоков данных, с целью получения конфиденциальной информации.
- Вмешательство в процесс функционирования ИС со стороны сетей общего пользования с целью несанкционированной модификации данных, доступа к конфиденциальной информации, навязывания ложной информации, провоцирования перегрузки ресурсов и сервисов.

Наличие не блокированных специальными мерами угроз информационной безопасности (уязвимостей) само по себе не причиняет материального ущерба владельцу информационных активов. Попытку реализовать уязвимость объекта информатизации со злонамеренными целями осуществляют нарушители информационной безопасности.

# 7. Модель нарушителя

## 7.1. Классификация нарушителей ИБ

Под нарушителем информационной безопасности понимается субъект, действия которого направлены на реализацию угроз информационной безопасности.

Попытка реализации угроз с целью нанесения ущерба информационным ресурсам называется атакой. Атака может быть осуществлена как непосредственно нарушителем, так и рядом инициированных им процессов, выполняемых программно-аппаратными средствами.

СОИБ Компании должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

Нарушитель ИБ характеризуется следующими параметрами:

- Цели проведения атаки.
- Правоотношение к объекту атаки.
- Квалификация и аналитические возможности.
- Техническая оснащенность.

Среди целей проведения атаки основными являются:

- любопытство;
- тренировка и проверка своих навыков и возможностей по преодолению защиты объектов информатизации;
- получение материальной выгоды;
- получение доступа к конфиденциальной информации с целью дальнейшего ее использования в корыстных целях;
- нанесение материального и репутационного ущерба компании.

Кроме того, отдельно выделяются действия (или бездействие) сотрудников, не преследующие ни одной из вышеперечисленных целей, а порожденные низкой квалификацией или халатным отношением к своим обязанностям.

Возможны следующие правоотношения нарушителя ИБ с объектом защиты информации:

- сотрудник, имеющий в соответствии со своими функциональными обязанностями непосредственный доступ к информационным активам Компании;

- сотрудник, имеющий в соответствии со своими функциональными обязанностями, доступ к смежным объектам;
- Клиенты и партнеры Компании, имеющие в соответствии с договорными отношениями доступ к информационным активам Компании;
- субъекты (отдельные физические лица и их группы, юридические лица), не имеющие юридически оформленных правоотношений по отношению к объекту информатизации.

По уровню квалификации и аналитическим возможностям выделяются следующие уровни подготовленности нарушителей:

- Высокая квалификация. Данный уровень нарушителя характеризуется глубокими знаниями принципов построения, функционирования и программно-технической реализации объекта атаки, а также возможных механизмов защиты и методов их преодоления.
- Уровень квалификации выше среднего. Он характеризуется наличием у нарушителя знаний и навыков, достаточных для эксплуатации объекта атаки, и методов его защиты.
- Средняя квалификация. Данный уровень характеризуется наличием у нарушителя общих знаний об объекте атаки и методах защиты.
- Уровень квалификации ниже среднего. Данный уровень характеризуется наличием у нарушителя общих знаний о принципах функционирования объекта атаки.
- Низкая квалификация. Данный уровень характеризуется отсутствием знаний о принципах функционирования объектов информатизации и средств защиты информации.

По уровням технической оснащенности нарушители подразделяются:

- высокий уровень: нарушитель оснащен сложными дорогостоящими программно-техническими комплексами;
- уровень нарушителя выше среднего: нарушитель оснащен специальными программно-техническими средствами;
- средний уровень: нарушитель использует свободно распространяемое ПО и общеупотребительные технические средства;
- нарушителя ниже среднего: нарушитель использует подручные средства;
- низкий уровень: нарушитель специального оснащения не имеет и не использует.

В целях поддержания адекватной и эффективной системы защиты в условиях изменения угроз безопасности информации и информационных ресурсов и компонентов систем и сетей оценка и моделирование угроз и нарушителей ИБ осуществляется на систематической основе как на этапе создания систем и сетей, так и в ходе их эксплуатации, в том числе при развитии (модернизации) и оформляется в виде частных моделей угроз Компании или, при необходимости, отдельных ИС.

При построении СОИБ следует руководствоваться наиболее актуальными частными моделями угроз и нарушителей, а в случае отсутствия как соответствующей частной модели, так и конкретных данных о нарушителе, следует полагать, что предполагаемый нарушитель обладает возможностями, близкими к потенциально достижимым. При этом необходимо считать, что нарушитель обладает высокими профессиональными знаниями в области защиты информации и обеспечен необходимыми программно-техническими средствами, находится при необходимости в непосредственной близости к объекту информатизации. Кроме того, обладает исчерпывающими данными об объекте атаки.

7.2. Внутренние нарушители информационной безопасности

Сотрудники Компании имеют санкционированный доступ ко всей информационной сфере сети связи и реально могут своими действиями или бездействием негативно влиять на состояние безопасности информационных ресурсов и инфраструктуры сети связи. Мировой опыт показывает, что более 70% нарушений информационной безопасности происходит при непосредственном участии сотрудников компании.

Среди сотрудников Компании можно выделить следующих нарушителей ИБ:

7.2.1 Неквалифицированный сотрудник. Данная категория нарушителей не имеет каких-либо конкретных целей и осуществляет нарушения своими действиями или бездействием неумышленно из-за недостаточной профессиональной квалификации. Техническое оснащение нарушителя и квалификация имеют, как правило, низкий уровень. Тем не менее, уровень материального, ущерба, причиняемого неквалифицированным сотрудником в зависимости от его должности, может быть достаточно высоким.

7.2.2 Недобросовестный сотрудник. Данная категория нарушителей ИБ также осуществляет нарушения своими действиями или бездействием, но умышленно, нарушая свои должностные инструкции сознательно. При этом нарушитель может также не иметь конкретных целей, либо

реализовывать свое любопытство и проверять свои возможности по преодолению систем защиты. Техническое оснащение нарушителя имеет, как правило, средний уровень, а квалификация, как нарушителя ИБ, может достигать высокого уровня.

7.2.3 "Обиженный" сотрудник. Данная категория нарушителей может иметь различную профессиональную квалификацию, а среди целей нарушения ИБ основной является причинение своими действиями материального ущерба компании (из мести или самоутверждения). Техническое оснащение нарушителя может иметь уровень выше среднего, а квалификация, как нарушителя ИБ, может достигать высокого уровня.

7.2.4 Сотрудник, вступивший в сговор с преступными элементами и группами. Данная категория нарушителей может иметь различную профессиональную квалификацию, а среди целей нарушения ИБ основной является получение материальной выгоды. Техническое оснащение нарушителя может иметь уровень выше среднего или даже высокого, а квалификация, как нарушителя ИБ, может достигать высокого уровня.

Сотрудники Компании имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами или конкурентами.

7.3. Внешние нарушители информационной безопасности

Внешние нарушители информационной безопасности могут представлять собой как отдельных субъектов, так и группы, коллективы и т.д., объединенные одной целью – нанесение ущерба Компании. Другой особенностью внешних нарушителей является отсутствие бесконтрольного легального доступа к информационным активам и ИТ-инфраструктуре Компании.

К внешним нарушителям ИБ можно отнести следующие субъекты и их объединения:

- отдельные преступные элементы и криминальные структуры – представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников Компании всеми доступными им силами и средствами. Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в АС. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными сотрудниками Компании и криминальными структурами.
- проектировщики, поставщики оборудования и ПО, системные интеграторы информационных и технологических проектов – представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным активам. Криминальные структуры и конкуренты могут использовать эти организации для временного устройства на работу своих членов, с целью доступа к защищаемой информации Компании.
- недобросовестные конкуренты – представляют внешнюю угрозу в случае использования ими информационной сферы в целях завоевания позиций на рынке, привлечения клиентов и снижения имиджа Компании.
- недобросовестные продавцы услуг - нарушители ИБ этой группы преследуют цель – получение материальной выгоды за счет финансового мошенничества при предоставлении услуг.

При построении СОИБ принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия исключают возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий двух и более нарушителей – сотрудников Компании по преодолению системы защиты;
- нарушитель скрывает свои несанкционированные действия от других сотрудников Компании;
- несанкционированные действия могут быть следствием ошибок сотрудников, а также недостатков принятых процедур и технологий обработки, хранения и передачи информации;
- в своей противоправной деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей. При этом, если иное не предусмотрено частной

моделью угроз и нарушителя, угрозы, реализуемые посредством перехвата побочных электромагнитных излучений и наводок (ПЭМИН) следует считать неактуальными, так как для их реализации злоумышленник должен обладать высокой квалификацией, иметь в своём распоряжении дорогостоящую специальную технику и располагаться в непосредственной близости к ИС, что делает реализацию таких угроз экономически нецелесообразной относительно стоимости полученной информации.

## 8. Управление рисками

Под информационным риском понимается совокупность (произведение) вероятностей реализации угрозы ИБ в отношении какого-либо информационного актива и ущерба, который понесет Компания при ее реализации.
Для эффективного управления рисками в Компании должна быть проведена классификация информационных активов по степени конфиденциальности, целостности и доступности. Классификация информационных активов проводится их владельцами, которые в дальнейшем отвечают за поддержание этой классификации в актуальном состоянии, т.е. должны регулярно проверять правильность текущей классификации и своевременно классифицировать новые данные.

При оценке угрозы нарушения конфиденциальности учитываются:

- стоимость упущенной выгоды (потеря клиентов, кража продуктов, обесценивание акций, и т.д.);
- стоимость выплаты неустоек, штрафов за невыполнение обязательств, судебные издержки;
- стоимость затрат на восстановление репутации, престижа имиджа Компании; стоимость затрат на привлечение новых клиентов.

При оценке угрозы нарушения целостности учитываются:

- стоимость упущенной выгоды (от невозможности предоставления услуги или неадекватного функционирования информационной системы);
- расходы на восстановление информационного ресурса;
- расходы на создание информационного ресурса (затраты на производство).

При оценке угрозы нарушения доступности учитываются:

- стоимость упущенной выгоды от невозможности предоставления услуги;
- заработная плата сотрудников за время простоя;
- расходы на восстановление инфраструктуры, замену оборудования;
- расходы на восстановление работоспособности информационной системы (запуск резервной дублирующей системы);
- негативное влияние на имидж Компании.

Следует определить, по каким параметрам будет проводиться оценка стоимости информационных активов, а также перечень критериев для каждого параметра. На основании этих данных владелец определяет стоимость информационного актива, которая равна сумме ущербов, которые понесет Компания по каждому из критериев. При определении ущерба следует спрогнозировать ситуацию нарушения конфиденциальности, целостности или доступности информационного актива и определить последствия такого нарушения. Для удобства оценки следует ввести шкалу категорий по уровню возможного ущерба («высокий»/ «средний»/ «низкий»), определив диапазоны ущерба в материальном и нематериальном выражении для каждой из категорий.
Перечень возможных угроз и вероятности их реализации для каждого из информационных активов оценивается подразделением ИБ на основании опубликованной статистики, рекомендаций компетентных организаций и опыта.

Полученные результаты представляются руководству Компании, и в отношении их определяется один из возможных способов обработки риска:

- Принятие риска осуществляется в том случае, если уровень риска признается допустимым. Т.е. Компания не считает целесообразным применять какие-либо меры по отношению к этим рискам и готова понести ущерб.
- Уклонение от риска – полное устранение источника риска.
- Передача рисков – перенесение ответственности за риск на третьи лица (например, поставщику оборудования или страховой компании) без устранения источника риска.
- Снижение рисков – это внедрение мер по снижению вероятности нанесения ущерба.

Оценка и анализ рисков должны проводиться в Компании на регулярной основе с целью контроля действенности принятых мер и учета изменений в ИС, таких как:

- появление в Компании новых информационных активов;
- выявление новых уязвимостей;
- изменение вероятности реализации существующих уязвимостей.

Таким образом, управление рисками является непрерывным процессом, составляющим основу СОИБ Компании.

## 9. Принципы обеспечения информационной безопасности

Построение СОИБ Компании и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

### 9.1. Законность

Предполагает осуществление защитных мероприятий и разработку СОИБ в соответствии с действующим законодательством РФ в области информации, информатизации и защиты информации, других нормативных актов по безопасности информации, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры безопасности информации не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к информации конкретных систем.

Сотрудники Компании должны иметь представление об ответственности за правонарушения в области обработки информации.

### 9.2 Системность

Системный подход к построению СОИБ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы защиты информации.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

### 9.3 Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано.

### 9.4 Непрерывность защиты

Защита информации должна рассматриваться не как разовое мероприятие и не как совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС Компании, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

### 9.5 Своевременность

Предполагает упреждающий характер мер обеспечения ИБ. Постановка задач по защите информационных активов и их реализация должна проводиться на ранних стадиях разработки проектов и процессов, связанных с обработкой информации.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

### 9.6 Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИС и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

9.7 Разумная достаточность.

Предполагает соответствие уровня затрат на обеспечение безопасности ценности информационных активов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности не должны заметно ухудшать эргономические показатели работы сотрудников и технические параметры ИС, в которой эта информация циркулирует.

9.8 Персональная ответственность.

Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

9.9 Принцип минимизации полномочий.

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

9.10 Взаимодействие и сотрудничество.

Предполагает создание благоприятной атмосферы в коллективах подразделений Компании и понимания сотрудниками необходимости и значимости выполнения требований ИБ. В такой обстановке сотрудники должны осознанно соблюдать установленные правила обработки информации и оказывать содействие в деятельности подразделений, ответственных за обеспечение ИБ и эксплуатацию технических средств ИС.

9.11 Открытость алгоритмов и механизмов защиты.

Защита информации не должна обеспечиваться только за счет секретности структурной организации, алгоритмов и технологий функционирования ее подсистем. Знание принципов и деталей работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация о конкретной системе защиты должна быть общедоступна.

9.12 Простота применения средств защиты.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных технологий или с выполнением действий, требующих значительных дополнительных трудозатрат при работе сотрудников в штатном режиме.

9.13 Научная обоснованность и техническая реализуемость.

Технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития информационных технологий, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

9.14 Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации организаций, специализирующихся в области ИБ, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Компании (специалистами подразделений ИТ во взаимодействии со Службой безопасности Компании).

9.15 Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения ИБ.

Контроль действий любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

# 10 Меры защиты информации

10.1 Правовые (законодательные) меры защиты

К правовым мерам защиты относятся действующие в Российской Федерации законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

Правоотношения и ответственность за нарушение законодательства РФ в информационной сфере определяются Гражданским (ст. ст. 150, 152.1), Уголовным (ст. ст. 183, 272-274) кодексами РФ, Кодексом об административных правонарушениях (ст. ст. 13.11-13.14).

10.2 Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются в стране и обществе, а также нормы корпоративной культуры Компании. Эти нормы, как неписаные (например, общепризнанные нормы честности, лояльности и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний, большей частью не являются обязательными, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

10.3 Организационные (административные) меры защиты.

10.3.1 Политика ИБ.

Организационные (административные) меры защиты – это совокупность правил, процедур и регламентов (закрепленных в нормативных документах Компании), определяющих процессы обработки информации, деятельность сотрудников, таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или минимизировать ущерб в случае их реализации. Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политика ИБ Компании должна быть разделена на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Компании в целом. Примером таких решений могут быть:

- область применения политики безопасности информации;
- роли и обязанности должностных лиц, отвечающие за проведение политики безопасности информации;
- кто имеет права доступа к информации ограниченного распространения;
- кто и при каких условиях может читать и модифицировать информацию и т.д.

Политика нижнего уровня определяет процедуры и правила достижения конкретных целей и решения частных задач защиты информации и детализирует (регламентирует) эти правила.

10.3.2 Регламентация доступа в помещения ИС Компании.

Эксплуатация технических средств, принадлежащих ИС Компании должна осуществляться в помещениях, оборудованных надежными автоматическими замками, средствами сигнализации и/или контроля доступа, постоянно находящимися под охраной или

наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (ПК, документов, реквизитов доступа и т.п.).

Уборка помещений с установленным в них серверным и телекоммуникационным оборудованием должна производиться в присутствии ответственного, за которым закреплены данные технические средства, или сотрудника охраны объекта с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами и металлическими шкафами.

Помещения должны быть обеспечены средствами уничтожения документов.

10.3.3 Регламентация допуска сотрудников к использованию ресурсов ИС Компании.

В рамках разрешительной системы допуска устанавливается:

- кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях;
- система разграничения доступа, которая предполагает определение для всех пользователей АС информационных и программных ресурсов, доступных им для конкретных операций (чтение, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

Допуск сотрудников подразделений Компании к работе с информационными активами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем ИС должны производится на основании заявки от руководителя подразделения. Заявка должна быть согласована (авторизована) с владельцем информационного ресурса и подразделением информационной безопасности.

Каждый сотрудник (при приеме на работу) должен подписывать Соглашение -обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению коммерческой тайны, а также правил работы с защищаемой информацией.

Обработка защищаемой информации в подсистемах ИС Компании должна производиться в соответствии с утвержденными технологическими инструкциями (техническими порядками) для данных подсистем.

Распределение имен, генерация паролей, модификация правил разграничения доступа к базам данных возлагается на специальных пользователей - администраторов конкретных баз данных. При этом могут использоваться, как только штатные, так и дополнительные средства защиты СУБД и операционных систем.

10.3.4 Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИС Компании.

Аппаратно-программная конфигурация ПК, на которых обрабатывается защищаемая информация, должна соответствовать кругу возложенных на пользователей данного ПК функциональных обязанностей. Все неиспользуемые в работе устройства ввода-вывода информации на них должны быть отключены (удалены), не нужные для работы программные средства и данные также должны быть удалены.

Для упрощения сопровождения, обслуживания и организации защиты ПК должны оснащаться программными средствами и конфигурироваться унифицировано (в соответствии с установленными правилами).

Все программное обеспечение (разработанное специалистами Компании, полученное централизованно или приобретенной у производителей) должно установленным порядком проходить тестирование и передаваться в архив программного обеспечения Компании. В подсистемах ИС должны устанавливаться и использоваться только взятые из архива программные средства. Использование неучтенного ПО должно быть запрещено.

Порядок разработки ПО, проведения тестирования, разработанного и приобретенного ПО, передача ПО в эксплуатацию должен быть регламентирован.

10.3.5 Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов ИС Компании.

Узлы и блоки телекоммуникационного и серверного оборудования, к которым доступ обслуживающего персонала в процессе эксплуатации не требуется, а также системные блоки ПК, после наладочных, ремонтных и иных работ, связанных со вскрытием их корпусов, должны закрываться и\или опечатываться (пломбироваться) уполномоченными сотрудниками Департамента ИТ Компании. Системные блоки ПЭВМ пользователей также

должны быть закрыты и\или опечатаны уполномоченными сотрудниками Департамента ИТ, а в случаях, когда их присутствие не представляется возможным.

Повседневный контроль за целостностью) на системных блоках ПЭВМ должен осуществляться пользователями ПК, периодический контроль - сотрудниками Отдела информационной безопасности.

10.3.6 Кадровая работа (подбор и подготовка персонала, обучение пользователей).

До начала работы с информацией сотрудники Компании должны быть ознакомлены с перечнем сведений, подлежащих защите, в части их касающейся, и своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации ограниченного распространения.

Защита информации по всем перечисленным направлениям возможна только после выработки у пользователей определенной дисциплины, т.е. норм, обязательных для исполнения всеми, кто работает с информационными активами. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу ИС Компании, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей.

Все сотрудники Компании, использующие при работе конкретные ИС, должны быть ознакомлены с организационно-распорядительными документами по их защите, должны знать и неукоснительно выполнять технологические инструкции.

Одним из направлений кадровой работы должно быть повышение осведомленности сотрудников в области ИБ (в том числе с периодической имитацией реализации угроз и проведения киберучений), разъяснения им норм и требований по безопасности, своевременного оповещения об изменениях в организационно-распорядительных документах.

10.4 Физические меры защиты.

Физические меры защиты основаны на применении механических, и/или электронно-механических средств, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации.

Для обеспечения физической безопасности компонентов ИС Компании необходимо осуществить ряд организационных и технических мероприятий, включающих:

организацию системы охранно-пропускного режима и системы контроля допуска на объект;

- введение дополнительных ограничений по доступу в помещения, предназначенные для размещения серверного и технологического оборудования, для хранения и обработки конфиденциальной информации;
- оборудование объектов информатизации устройствами защиты от сбоев электропитания и помех в линиях связи (источниками бесперебойного электропитания);
- визуальный и технический контроль контролируемой зоны объекта защиты;
- оборудование объектов информатизации системами климатического контроля;
- оборудование объектов информатизации системами противопожарной сигнализации и автоматического пожаротушения.

10.5 Технические меры защиты.

Технические меры защиты основаны на использовании различного оборудования и программных средств, входящих в состав ИС Компании и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты информации.

С учетом всех требований и принципов обеспечения безопасности информации в состав системы защиты должны быть включены следующие средства:

- средства аутентификации пользователей и элементов ИС Компании, соответствующих степени конфиденциальности информации и обрабатываемых данных;
- средства разграничения доступа к данным;
- средства криптографической защиты информации в каналах передачи данных и в базах данных;
- средства регистрации обращений и контроля использования защищаемой информации;
- средства регистрации, мониторинга и реагирования на инциденты информационной безопасности;
- средства межсетевого экранирования;
- средства реагирования на обнаруженный НСД;
- средства обнаружения и уничтожения вредоносных программных кодов (антивирусное ПО);
- средства анализа защищенности системы;
- средства обнаружения атак.

На технические средства ЗИ возлагается решение следующих основных задач:

- идентификация и аутентификации пользователей при помощи имен, паролей и/или специальных аппаратных средств (e-token, securID и т.п.) и/или неотъемлемых характеристик пользователей (как правило – биометрических);
- разграничение доступа пользователей к периферийным устройствам компьютера;
- полномочное разграничение доступа к защищаемым данным на ПК и на файловых ресурсах в соответствии с ролевой моделью разграничения доступа;
- создание замкнутой программной среды разрешенных для запуска программ, расположенных как на локальных, так и на сетевых дисках;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- контроль целостности модулей системы защиты, системных областей диска и произвольных списков файлов в автоматическом режиме и по командам администратора;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;
- централизованный сбор, хранение и обработка системных журналов регистрации событий;
- централизованное управление настройками средств разграничения доступа на ПК;
- оповещение администраторов безопасности обо всех событиях НСД, происходящих на рабочих станциях;
- оперативный контроль за работой пользователей сети, изменение режимов функционирования рабочих станций и возможность блокирования (при необходимости) любой станции сети.

Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными мерами и используемыми физическими средствами защиты:

- физическая целостность всех компонент ИС Компании обеспечена;
- каждый сотрудник (пользователь системы) имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- использование на рабочих станциях ИС Компании инструментальных и технологических программ (тестовых утилит, отладчиков и т.п.), позволяющих предпринять попытки взлома или обхода средств защиты, ограничено и строго регламентировано;
- в защищенной системе нет программирующих пользователей. Разработка и отладка программ осуществляется за пределами защищенной системы;
- все изменения конфигурации технических и программных средств ИС производятся строго установленным порядком только на основании распоряжений руководства структурных подразделений Компании;
- телекоммуникационное оборудование располагается в помещениях и местах, недоступных для посторонних лиц.
- Департаментом ИТ осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

10.5.1 Средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей

В целях предотвращения работы с ИС Компании посторонних лиц необходимо обеспечить возможность распознавания системой каждого законного пользователя (или ограниченных

групп пользователей). Для этого в системе (в защищенном месте) должен храниться ряд признаков каждого пользователя, по которым этого пользователя можно опознать. В дальнейшем при входе в систему, а при необходимости - и при выполнении определенных действий в системе, пользователь обязан себя идентифицировать, т.е. указать идентификатор, присвоенный ему в системе. Кроме того, для идентификации могут применяться различного рода устройства или биометрические параметры пользователя.

10.5.2 Средства разграничения доступа зарегистрированных пользователей к ресурсам ИС.

СЗИ должна осуществлять авторизацию пользователя, то есть определять, какие права предоставлены пользователю: какие данные и как он может использовать, какие программы может выполнять, когда, как долго и с каких терминалов может работать, какие ресурсы системы может использовать и т.п. Авторизация пользователя должна осуществляется с использованием следующих механизмов:

- механизмов избирательного управления доступом, основанных на использовании атрибутных схем, списков разрешений и т.п.;
- механизмов полномочного управления доступом, основанных на использовании меток конфиденциальности ресурсов и уровней допуска пользователей;
- механизмов обеспечения замкнутой среды доверенного программного обеспечения (индивидуальных для каждого пользователя списков разрешенных для запуска программ), поддерживаемых механизмами идентификации (распознавания) и аутентификации (подтверждения подлинности) пользователей при их входе в систему.

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны быть составной частью единой системы контроля доступа:

- на контролируемую территорию;
- в отдельные помещения;
- к элементам ИС и элементам системы защиты информации (физический доступ);
- к информационным хранилищам (носителям информации, томам, файлам, наборам данных, архивам, справкам, записям и т.д.);
- к активным ресурсам (прикладным программам, задачам, формам запросов и т.п.);
- к операционной системе, системным программам и программам защиты и т.п.

10.5.3 Средства обеспечения и контроля целостности программных и информационных ресурсов

Контроль целостности программ, обрабатываемой информации и средств защиты, с целью обеспечения неизменности программной среды и защиты от несанкционированной корректировки информации должен обеспечиваться:

- средствами подсчета контрольных сумм;
- средствами электронной цифровой подписи;
- средствами сравнения критичных ресурсов с их эталонными копиями (и восстановления в случае нарушения целостности);
- средствами разграничения доступа (запрет доступа с правами модификации или удаления).

В целях защиты информации и программ от несанкционированного уничтожения или искажения необходимо обеспечить:

- избыточность данных при хранении на дисках;
- отслеживание транзакций;
- антивирусный контроль;
- резервное копирование данных по заранее установленной схеме;
- хранение резервных копий за пределами технологических помещений, в которых размещено серверное оборудование;
- обеспечение непрерывности электропитания для серверного оборудования и критичных рабочих станций и кондиционирование электропитания для остальных станций сети.

Установка специализированного ПО, позволяющего корректно завершать работу прикладных задач и операционных систем серверов и рабочих станций в случае длительных перебоев электроснабжения.

10.5.4 Средства оперативного контроля и регистрации событий безопасности.

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение политики безопасности и привести к возникновению кризисных ситуаций.

Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов). Журналы регистрации должны вестись для каждой рабочей станции сети;
- оперативного ознакомления администратора безопасности с содержимым системного журнала любой станции и с журналом оперативных сообщений об НСД;
- получения твердой копии (печати) системного журнала;
- упорядочения системных журналов по дням и месяцам, а также установления ограничений на срок их хранения;
- оперативного оповещения администратора безопасности о нарушениях.

При регистрации событий безопасности в системном журнале должна фиксироваться следующая информация:

- дата и время события;
- идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
- действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

Средства контроля должны обеспечивать обнаружение и регистрацию следующих событий:

- вход (регистрация) пользователя в систему;
- неудачная попытка входа в систему или сеть (неправильный ввод пароля);
- запуск программы;
- завершение программы;
- попытка открытия файла недоступного для чтения;
- попытка открытия на запись файла недоступного для записи;
- попытка удаления файла недоступного для модификации;
- попытка изменения атрибутов файла недоступного для модификации;
- попытка запуска программы, недоступной для запуска;
- попытка получения доступа к недоступному каталогу;
- попытка чтения/записи информации с диска, недоступного пользователю;
- попытка запуска программы с диска, недоступного пользователю;
- нарушение целостности программ и данных системы защиты.

Должны поддерживаться следующие основные способы реагирования на обнаруженные факты НСД (возможно с участием администратора безопасности):

- извещение владельца информации о НСД к его данным;
- снятие программы (процесса) с дальнейшего выполнения;
- извещение системных администраторов и администраторов безопасности;
- отключение терминала (рабочей станции), с которого были осуществлены попытки НСД к информации;
- исключение нарушителя из списка зарегистрированных пользователей.

10.5.5 Криптографические средства защиты информации

Одним из элементов СОИБ Компании должно быть использование криптографических методов и средств защиты информации от несанкционированного доступа при ее хранении и передаче по незащищенным каналам связи.

Конфиденциальность информации при ее передаче по каналам связи должна обеспечиваться за счет применения в системе средств абонентского и на отдельных направлениях канального шифрования. Сочетание абонентского и канального шифрования информации должно обеспечивать ее сквозную защиту по всему тракту прохождения, защищать информацию в случае ее ошибочной переадресации за счет сбоев и неисправностей телекоммуникационного оборудования.

В качестве средств криптографической защиты конфиденциальной информации должны применяться аппаратно-программные средства, реализующие механизмы построения

виртуальных частных сетей (VPN) и использующие стандартизованные в международных информационных сетях алгоритмы и протоколы.

В ИС Компании, также должны использоваться средства формирования и проверки электронной цифровой подписи, обеспечивающие целостность и юридически доказательное подтверждение подлинности информации, а также аутентификацию пользователей и абонентских пунктов, являющихся ее отправителями. При этом должны использоваться только стандартизованные алгоритмы цифровой подписи, а соответствующие средства, реализующие эти алгоритмы, должны быть сертифицированы в РФ.

## 11 Контроль эффективности системы защиты

Контроль эффективности защиты информации осуществляется с целью обеспечения уверенности в том, что СОИБ функционирует надлежащим образом и для своевременного выявления уязвимостей конфигурации и реализации СЗИ.

Контроль должен проводиться как непосредственно специалистами Компании (самоконтроль, внутренний аудит, контроль со стороны Руководства Компании), так и привлекаемыми ею для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности (внешний аудит).

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты информации от НСД, так и с помощью специальных программных средств контроля.

## 12 Ответственность

Любое грубое нарушение порядка и правил работы с информацией сотрудниками Компании должно расследоваться. К виновным должны применяться адекватные меры воздействия. Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной обработки информации, должна определяться нанесенным ущербом, наличием злого умысла и прецедентов подобных нарушений, и другими факторами по усмотрению руководства Компании