УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[ИБ-100]

2018г.

Оглавление

1. Аннотация

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

- Основные принципы формирования перечня критичных ресурсов, нуждающихся в защите, формируемого в процессе проведения аудита безопасности и анализа рисков. Данный перечень должен включать в себя описание физических, программных и информационных ресурсов с определением стоимости ресурсов и степени их критичности для Компании.
- Основные принципы защиты, определяющие стратегию обеспечения информационной безопасности (ИБ) и перечень политик правил, которыми необходимо руководствоваться при построении системы обеспечения информационной безопасности (СОИБ) Компании.
- Модель нарушителя безопасности, определяемую на основе обследования ресурсов Компании и способов их использования.
- Модель угроз 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 безопасности, определяемые по результатам анализа рисков.
- Меры обеспечения безопасности организационного и программно-технического уровня, предпринимаемые для реализации требований безопасности.
- Ответственность сотрудников Компании за соблюдение установленных требований ИБ при эксплуатации информационных систем (ИС) Компании.

2. Общие положения

2.1. Назначение и правовая основа документа

Концепция информационной безопасности (далее – Концепция) Компании определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, а также требований и базовых подходов к их реализации. В Концепции описывается общая стратегия обеспечения информационной безопасности Компании.

Методологической основой Концепции являются Российские и международные стандарты в области информационной безопасности.

Законодательной основой Концепции являются: Конституция Российской Федерации, Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации.

Концепция учитывает современное состояние и ближайшие перспективы развития информационных технологий в Компании, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений.

Основные положения Концепции базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

Концепция является методологической основой для:

- формирования Политики информационной безопасности в Компании;
- выработки комплекса согласованных мер по выявлению, отражению и нейтрализации угроз безопасности информации;

- координации деятельности структурных подразделений Компании и ответственных лиц при проведении работ по созданию, развитию и эксплуатации информационных технологий;
- разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения Политики информационной безопасности Компании.

Положения и требования Концепции распространяются на все структурные подразделения, входящие в состав Компании.

2.2. Объекты защиты

Основными объектами системы информационной безопасности Компании являются:

1. Информационные ресурсы, содержащие сведения, составляющие коммерческую тайну, или иные критичные информационные ресурсы Компании;
2. Процессы обработки, хранения и передачи информации в информационной системе Компании, а также ее участники (пользователи и обслуживающий персонал);
3. Инфраструктура информационной системы Компании (технические и программные средства анализа, обработки, передачи и отображения, каналы информационного обмена и телекоммуникации, объекты и помещения, в которых они размещены);
4. Структура, состав и размещение средств защиты информации, их взаимодействие с информационной системой и точки подключения к ней;
5. Открытая (общедоступная) информация, необходимая для работы Компании, независимо от формы и вида ее представления.

Информационная среда Компании является распределенной структурой, объединяющей различные информационные системы. К основным особенностям информационной среды Компании относятся:

- Территориальная распределенность компонентов информационной системы;
- Объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;
- Большое разнообразие решаемых задач и типов обрабатываемых данных, сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов различных пользователей;
- Важность и ответственность решений, принимаемых на основе автоматизированной обработки данных;
- Абстрагирование владельцев информации от физических структур и места размещения информации;
- Наличие большого числа информационных каналов взаимодействия с «внешним миром» (источниками и потребителями информации);
- Высокая интенсивность информационных потоков;
- Разнообразие категорий пользователей и обслуживающего персонала информационной системы.

В этих условиях резко возрастают требования, предъявляемые к информационной среде, и в частности - к информационной системе Компании, в которой обрабатываются и накапливаются значительные объемы информации.

2.3. Категории информационных ресурсов, подлежащих защите

В информационной системе Компании циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (государственная, коммерческая или служебная тайна, персональные данные) и открытые сведения.

Защите подлежит вся информация, обрабатываемая информационной системой Компании, независимо от ее представления и местонахождения в информационной среде, относящаяся к следующим категориям:

- Сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации в соответствии с Федеральным законом «О коммерческой тайне»;
- Служебная информация, угроза безопасности которой может негативно повлиять на деятельность Компании;
- Открытая информация, необходимая для обеспечения бизнес-процессов Компании;
- Интересы затрагиваемых субъектов информационных отношений.

Субъектами информационных отношений Компании являются:

- Структурное подразделение Компании или лица, являющиеся владельцами информационных ресурсов;
- Подразделения Компании, участвующие в информационном обмене;
- Сотрудники Компании, в соответствии с возложенными на них функциями;
- Юридические и физические лица, сведения о которых присутствуют в информационной системе Компании;
- Другие юридические и физические лица, прямо или косвенно задействованные в бизнес-процессах Компании (консультанты, разработчики, обслуживающий персонал, организации, привлекаемые для оказания услуг и пр.).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- Своевременного доступа к необходимой информации (ее доступности);
- Достоверности (полноты, точности, адекватности, целостности) информации;
- Конфиденциальности (сохранения в тайне) определенной части информации;
- Защиты от навязывания ложной (недостоверной, искаженной) информации;
- Ответственности за нарушения прав (интересов) и установленных правил обращения с информацией;
- Возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- Защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.).

2.4. Цели обеспечения безопасности информации

Целями обеспечения безопасности информации являются:

- Защита субъектов информационных отношений Компании от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи;
- Минимизация уровня рисков (операционные риски, риск нанесения урона деловой репутации Компании, правовой риск и т.д.).

Указанные цели достигаются посредством обеспечения и постоянного поддержания следующих свойств информации:

- Доступность информации для легальных пользователей (устойчивого функционирования информационной системы Компании, при котором пользователи имеют возможность своевременного получения необходимой информации);
- Целостность и аутентичность (подтверждение авторства) информации, хранимой, обрабатываемой и передаваемой в информационной системе Компании;
- Конфиденциальность определенной части информации, хранимой, обрабатываемой и передаваемой в информационной системе Компании.

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается соответствующими методами и средствами.

2.5. Задачи обеспечения безопасности информации

Для достижения целей защиты и обеспечения указанных свойств информации система информационной безопасности Компании должна обеспечивать эффективное решение следующих задач:

- Своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы Компании;
- Создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- Создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и оперативная ликвидация последствий нарушения безопасности информации;
- Защита от утечки (несанкционированного разглашения и ознакомления), разрушения (несанкционированного уничтожения), блокирования (несанкционированного ограничения) или искажения (несанкционированной модификации) информации и контроль целостности используемых в информационной системе Компании программных средств, а также защита информационной системы от внедрения вредоносных программ;
- Защита от вмешательства в процесс функционирования информационной системы Компании посторонних лиц (доступ к информационным ресурсам должны иметь только авторизованные в установленном порядке пользователи);
- Разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Компании (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
- Обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- Регистрация действий пользователей при использовании защищаемых ресурсов информационной системы Компании в системных журналах и периодический контроль корректности действий пользователей системы;
- Обеспечение надежности криптографических средств защиты информации.

2.6. Основные пути решения задач защиты информации

Поставленные основные цели защиты информации и решение перечисленных выше задач достигаются:

- Строгим учетом всех подлежащих защите ресурсов информационной системы Компании (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- Регламентацией процессов обработки информации и действий пользователей;
- Регламентацией действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;

- Полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Компании по вопросам обеспечения безопасности информации;
- Назначением и подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;
- Наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Компании;
- Четким знанием и строгим соблюдением всеми пользователями информационной системы Компании требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- Персональной ответственностью за свои действия каждого сотрудника, имеющего доступ к информационным ресурсам Компании;
- Принятием эффективных мер обеспечения физической целостности компонентов информационной системы и непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Компании;
- Применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- Разграничением потоков информации, предусматривающим предупреждение попадания информации более высокого уровня конфиденциальности на информационные ресурсы с более низким уровнем конфиденциальности, а также запрещением передачи конфиденциальной информации по незащищенным каналам связи;
- Эффективным контролем над соблюдением пользователями информационных ресурсов Компании требований по информационной безопасности;
- Юридической защитой интересов Компании при информационном взаимодействии его подразделений с внешними организациями от противоправных действий, как со стороны этих организаций и третьих лиц, так и со стороны Компании;
- Проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты информации в информационной системе Компании.

2.7. Угрозы безопасности информации и их источники

Все множество потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные). Естественные угрозы – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека. Искусственные угрозы – это угрозы, вызванные деятельностью человека. Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

Основными источниками угроз безопасности информации являются:

- Непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки, хранения и передачи информации, а также требований безопасности информации и другие действия пользователей информационной системы Компании (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и

ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы Компании;

- Преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам Компании пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы Компании;
- Деятельность преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности информационной системы Компании в целом или ее отдельных компонент;
- Удаленное несанкционированное вмешательство посторонних лиц из территориально удаленных сегментов корпоративной информационной системы и внешних сетей общего назначения (прежде всего Интернет) через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам;
- Ошибки, допущенные при разработке компонентов информационной системы и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты);
- Аварии, стихийные бедствия.

Наиболее значимыми угрозами безопасности информации Компании (способами нанесения ущерба субъектам информационных отношений) являются:

- Нарушение функциональности компонентов информационной системы Компании, блокирование информации, нарушение бизнес-процессов, срыв своевременного решения задач;
- Нарушение целостности (искажение, подмена, разрушение) информационных, программных и других ресурсов;
- Нарушение конфиденциальности (разглашение, утечка) сведений, составляющих государственную, коммерческую или служебную тайну, а также персональных данных.

2.8. Пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации

Сотрудники Компании, зарегистрированные как легальные пользователи информационной системы Компании или обслуживающие ее компоненты, могут являться внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к информационным ресурсам и процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и регламентов.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации Компании:

- Неосторожные или халатные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;
- Разглашение, передача или утрата атрибутов разграничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т. п.);

- Игнорирование установленных организационных правил при работе с информационными ресурсами;
- Неквалифицированное проектирование архитектуры систем, технологий обработки данных или неквалифицированная разработка программного обеспечения, повлекшая за собой возникновение возможностей, представляющих опасность для функционирования информационной системы и безопасности информации;
- Ошибочная адресация при передаче или пересылке информации;
- Ввод ошибочных данных;
- Неумышленная порча носителей информации;
- Неумышленное повреждение каналов связи;
- Неквалифицированное (ошибочное) отключение оборудования или изменение режимов работы устройств или программ;
- Заражение компьютеров вирусами вследствие халатности пользователя;
- Неквалифицированное использование программного обеспечения, способного вызвать потерю работоспособности компонентов корпоративной информационной системы или осуществляющего необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- Некомпетентное использование, настройка или отключение средств защиты.

2.9. Пути реализации преднамеренных искусственных (субъективных) угроз безопасности информации

Основные возможные пути умышленной дезорганизации работы, вывода компонентов информационной системы Компании из строя, несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.):

- Умышленные действия, приводящие к частичному или полному нарушению функциональности информационной системы Компании или ее компонентов, в том числе умышленное разрушение информационных или программно-технических ресурсов;
- Хищение документов и носителей информации;
- Несанкционированное копирование информации;
- Умышленное искажение информации, ввод неверных данных;
- Отключение или вывод из строя подсистем обеспечения функционирования информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);
- Перехват данных, передаваемых по каналам связи;
- Хищение производственных отходов (распечаток документов, записей и т.п.);
- Незаконное получение и использование доступа к информационным ресурсам (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);
- Хищение или вскрытие шифров криптозащиты информации;
- Внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования компонентов информационной системы Компании;
- Незаконное использование оборудования, программных средств или информационных ресурсов, нарушающее права третьих лиц;
- Несанкционированное применение подслушивающих устройств, фото- и видеосъемка;
- Несанкционированный перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений

технических средств, непосредственно не участвующих в информационном обмене (сети питания).

2.10. Пути реализации основных естественных угроз безопасности информации

К естественным угрозам безопасности информации относятся:

- Выход из строя оборудования информационных систем и оборудования обеспечения его функционирования, не вызванный воздействиями извне и возникший по причине технической неисправности оборудования;
- Выход из строя или невозможность использования линий связи, не вызванный воздействиями извне и возникший по причине технической неисправности;
- Пожары, землетрясения, наводнения и другие стихийные бедствия.

2.11. Неформальная модель возможных нарушителей

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

1. Некомпетентный (невнимательный) пользователь – сотрудник Компании (или подразделения другой организации, являющийся легальным пользователем информационной системы Компании), который может предпринимать попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационной системы с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.п., действуя по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только доступные ему штатные средства.
2. Нарушитель - сотрудник Компании (или подразделения другой организации, являющийся зарегистрированным пользователем информационной системы Компании), пытающийся нарушить систему защиты без корыстных целей или злого умысла. Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого, он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства.
3. Внутренний злоумышленник - сотрудник Компании (или подразделения другого ведомства, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов, целей вредительства или любопытства, возможно в сговоре с лицами, не являющимися сотрудниками Компании. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Компании.
4. Внешний злоумышленник – лицо, не являющееся сотрудником Компании, действующее целенаправленно из корыстных интересов, целей вредительства или любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы,

пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Компании.

Внутренним нарушителем может быть лицо из следующих категорий:

- Зарегистрированные пользователи информационной системы Компании;
- Сотрудники Компании, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационной системы Компании, но имеющие доступ в здания и помещения Компании;
- Персонал, обслуживающий технические средства корпоративной информационной системы;
- Персонал, задействованный в разработке и сопровождении программного обеспечения.

Категории лиц, которые могут быть внешними нарушителями:

- Уволенные сотрудники Компании;
- Представители организаций, взаимодействующих по вопросам технического обеспечения Компании;
- Клиенты Компании;
- Посетители (представители организаций, поставляющих технику, программное обеспечение, услуги и т.п.);
- Представители конкурирующих организаций;
- Члены организованных преступных группировок, сотрудники спецслужб или лица, действующие по их заданию;
- Лица, случайно или умышленно проникшие в информационную систему Компании из внешних телекоммуникационных сетей.

Пользователи и обслуживающий персонал из числа сотрудников Компании имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к информационным ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связаны с нарушением действующих правил и инструкций.

Особую категорию составляют администраторы и менеджеры различных автоматизированных систем, имеющих практически неограниченный доступ к информационным ресурсам корпоративной информационной системы. Численность данной категории пользователей должна быть минимальной, а их действия должны находиться под обязательным контролем подразделения безопасности.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, мерах защиты информации, правах и способах доступа к информационным ресурсам Компании. Полученные во время работы в Компании знания и опыт выделяют их среди других источников внешних угроз.

Криминальные структуры являются наиболее агрессивным источником 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 взломщики имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в автоматизированных системах обработки информации. Они представляют наибольшую угрозу при взаимодействии с работающими или уволенными сотрудниками Компании и криминальными структурами.

Организации, занимающиеся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Конкурирующие организации, криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов с целью доступа к ресурсам информационной системы Компании.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- Нарушитель скрывает свои несанкционированные действия от других сотрудников Компании;
- Несанкционированные действия могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- В своей 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.

2.12. Утечка информации по техническим каналам

При проведении мероприятий и эксплуатации технических средств возможны следующие каналы утечки или искажения информации, нарушения работоспособности технических средств:

- Побочные электромагнитные излучения технических средств и линий передачи информации;
- Наводки информативного сигнала, обрабатываемого техническими средствами корпоративной информационной системы, на провода и линии, выходящие за пределы контролируемой зоны, в т.ч. на цепи заземления и электропитания;
- Электрические сигналы или радиоизлучения, обусловленные воздействием на средства передачи информации высокочастотных сигналов, создаваемых с помощью специальной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.) и модуляцией их информативным сигналом;
- Радиоизлучения или электрические сигналы от внедренных в помещения специальных электронных устройств перехвата информации («закладок»), модулированные информативным сигналом;
- Радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- Акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;
- Электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;
- Вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации;
- Просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств;
- Воздействие на технические или программные средства в целях нарушения целостности (разрушение, искажение) информации, работоспособности технических

средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедренные электронные и программные средства («закладки»).

Перехват информации или воздействие средства ее обработки, хранения и передачи может вестись непосредственно из зданий, расположенных в непосредственной близости от объектов Компании, мест временного пребывания, заинтересованных в перехвате или искажении информации лиц при посещении ими подразделений Компании, а также с помощью скрытно устанавливаемой аппаратуры.

В качестве аппаратуры разведок или воздействия на информацию и технические средства могут использоваться:

- Средства для перехвата радиоизлучений от средств радиосвязи и радиорелейных станций, а также приема сигнала от автономных автоматических средств разведки и электронных устройств перехвата информации («закладок»);
- Стационарные средства, размещаемые в зданиях;
- Мобильные специальные средства;
- Автономные средства, скрытно устанавливаемые на объектах защиты или поблизости от них.

Стационарные средства обладают наибольшими энергетическими, техническими и функциональными возможностями. В то же время они, как правило, удалены от объектов защиты и не имеют возможности подключения к линиям, коммуникациям и сооружениям. Мобильные средства могут использоваться непосредственно на объектах защиты или поблизости от них и могут подключаться к линиям и коммуникациям, выходящим за пределы контролируемой территории.

Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны. Такого рода утечка информации возможна вследствие:

- Непреднамеренного прослушивания без использования технических средств разговоров, ведущихся в выделенном помещении, из-за недостаточной звукоизоляции его ограждающих конструкций, систем вентиляции и кондиционирования;
- Случайного прослушивания телефонных переговоров при проведении профилактических работ на АТС, кроссах, кабельных коммуникациях с помощью контрольной аппаратуры;
- Просмотра информации с экранов дисплеев и других средств ее отображения.

3. Основные принципы обеспечения информационной безопасности

Построение системы безопасности информации и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность (экономическая целесообразность);
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- простота применения средств защиты;

- обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

3.1. Законность

Предполагает осуществление защитных мероприятий и разработку Политики информационной безопасности Компании в соответствии с действующим законодательством в области информации, информатизации и защиты информации, других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции, 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 подсистем.

Все пользователи информационной системы Компании должны иметь представление об ответственности за правонарушения в области информации.

Реализация данного принципа необходима для защиты имени и репутации Компании.

3.2. Системность

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

При создании системы защиты должны учитываться все уязвимые места информационной системы Компании, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

3.3. Комплексность

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

3.4. Непрерывность защиты

Обеспечение безопасности информации – постоянный процесс, осуществляемый руководством Компании, подразделением безопасности и сотрудниками всех уровней Компании. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности всех подразделений Компании.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе системы защиты информации могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления защиты.

3.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации на ранних стадиях разработки информационных систем в целом и их систем защиты информации в частности.

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

3.6. Преемственность и совершенствование

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

3.7. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение информационной безопасности ценности защищаемой информации и величине возможного ущерба от ее разглашения, утраты, утечки, блокирования или искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать функциональность компонентов информационной системы Компании. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности информации. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

3.8. Персональная ответственность

Предполагает возложение ответственности за обеспечение информационной безопасности на каждого сотрудника Компании в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников и степень их ответственности были четко определены.

3.9. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью по принципу «запрещено все, что не разрешено». Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

3.10. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах структурных подразделений Компании. В такой обстановке сотрудники должны осознанно соблюдать

установленные правила и оказывать содействие подразделениям, обеспечивающим режим безопасности информации.

Важным элементом эффективной Политики информационной безопасности является высокая культура работы с информацией. Руководители структурных подразделений Компании несут ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, за создание корпоративной культуры, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности. Все сотрудники Компании должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обращения с информацией не гарантирует автоматического достижения целей защиты информации, ее отсутствие или низкий уровень создают больше возможностей для нарушения безопасности или необнаружения фактов ее нарушения.

3.11. Гибкость системы защиты

Политика информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Компаниям своей деятельности. В число таких изменений входят:

- Изменения организационной и штатной структуры Компании;
- Корпоративная реструктуризация, слияния и поглощения;
- Расширение или приобретение бизнеса (включая влияние изменений в соответствующей экономической или правовой среде);
- Изменение существующих или внедрение принципиально новых информационных систем;
- Новые технические средства;
- Новые виды деятельности;
- Новые услуги, продукты.

Свойство гибкости системы информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

3.12. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

3.13. Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

3.14. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и

экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности информации.

3.15. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться специалистами, в чьи должностные обязанности входит обеспечение безопасности информации в Компании.

3.16. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью 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.

Кроме того, эффективная система информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с обработкой, хранением и передачей информации, и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы информационной безопасности, выявленные сотрудниками Компании или подразделениями безопасности должны своевременно доводиться до сведения руководителей соответствующего уровня и оперативно устраняться. Важно, чтобы после получения информации соответствующие руководители обеспечивали своевременное исправление недостатков. Руководство должно периодически получать отчеты, суммирующие все проблемы, выявленные системой информационной безопасности. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

4. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационной системы Компании подразделяются на:

- правовые (законодательные);
- морально-этические;
- технологические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

4.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране 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 информационной системы.

4.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в Компании. Эти нормы большей частью не являются обязательными как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или Компании в целом. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

4.3. Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии согласования нескольких лиц, процедур проверки реквизитов исходящих и входящих сообщений.

4.4. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

4.4.1. Формирование политики информационной безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать комплекс организационно-распорядительных документов (положений, регламентов, инструкций и т.д.), образующих Политику в области обеспечения безопасности информации (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

4.4.2. Регламентация доступа в помещения

Особо важные компоненты информационной системы Компании должны размещаться в помещениях, оборудованных надежными автоматическими замками, средствами сигнализации и постоянно находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, оборудования, реквизитов доступа и т.п.). Допуск в такие помещения должен производиться в присутствии ответственного, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

4.4.3. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы допуска устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.
Допуск пользователей к работе с информационной системой Компании и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком согласно регламенту предоставления доступа пользователей.

Основными пользователями информации в корпоративной информационной системе являются сотрудники структурных подразделений Компании. Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

- каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам в обязательном порядке должно согласовываться со структурным подразделением Компании, ответственным за информационное сопровождение данного ресурса;
- руководитель имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями;
- наиболее ответственные технологические операции должны производиться по правилу «в две руки» - правильность введенной информации подтверждается другим должностным лицом, не имеющим права ввода информации.

Все сотрудники Компании или других организаций несут персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы. В должностные инструкции каждого сотрудника обязательно включение задач по обеспечению информационной безопасности.

При приеме на работу сотрудники должны быть ознакомлены под роспись с перечнем информации, составляющей коммерческую или служебную тайну Компании, с установленным режимом работы с ней и с мерами ответственности за нарушение этого режима. Это делается в форме заключения с сотрудником отдельного соглашения о неразглашении конфиденциальной информации, действующее в период действия трудового договора и в течение трех лет с момента его прекращения.

Обработка информации в компонентах информационной системы Компании должна производиться в соответствии с утвержденными технологическими инструкциями.

4.4.4. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

Подлежащие защите ресурсы системы (документы и данные, оборудование, программное обеспечение) подлежат строгому учету (на основе использования соответствующих формуляров или специализированных баз данных).

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест (далее – АРМ), с которых возможен доступ к ресурсам корпоративной информационной системы, должна соответствовать кругу возложенных на пользователей функциональных обязанностей.

Ввод в эксплуатацию новых АРМ и все изменения в конфигурации существующих технических и программных средств должны осуществляться только в соответствии с утвержденными регламентами.

Все программное обеспечение (разработанное специалистами Компании, полученное централизованно или приобретенное у фирм-производителей) должно в установленном порядке

проходить испытания. Использование нелицензионного или не прошедшего проверку программного обеспечения, должно быть запрещено.

Разработка задач (комплексов задач), проведение испытаний разработанного или приобретенного программного обеспечения, и передача его в эксплуатацию должна осуществляться в соответствии с установленным порядком разработки, проведения испытаний и передачи задач (комплексов задач) в эксплуатацию.

4.4.5. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

На всех АРМ, подлежащих защите, должны быть установлены необходимые технические средства защиты (соответствующие категории данных АРМ).

Узлы и блоки вычислительной техники, доступ обслуживающего персонала к которым в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к их монтажным схемам должны закрываться и при необходимости опечатываться сотрудниками дирекции ИБ. На печати (пломбе) в обязательном порядке должна присутствовать дата пломбирования, фамилия и подпись лица, установившего ее. Печать (пломба) должна быть размещена так, чтобы вскрытие узла или блока без ее повреждения было бы невозможно.

Повседневный контроль за целостностью и соответствием печатей (пломб) на системных блоках ПЭВМ должен осуществляться пользователями и администраторами информационной системы. Периодический контроль - сотрудниками, ответственными за безопасность информации в Компании.

4.4.6. Подбор и подготовка персонала, обучение пользователей

Пользователи информационной системы Компании, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации.

Все пользователи информационной системы Компании должны быть ознакомлены с организационно-распорядительными документами по обеспечению информационной безопасности в части их касающейся, должны знать и неукоснительно выполнять регламенты, инструкции и общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

4.4.7. Подразделение информационной безопасности

Подразделение информационной безопасности состоит из сотрудников Дирекции по информационной безопасности и Департамента информационных технологий, в чьи должностные обязанности входит обеспечение безопасности информационной системы и режима коммерческой тайны в Компании.

Функции подразделения информационной безопасности заключаются в следующем:

- формирование требований к системам защиты информации в процессе создания и дальнейшего развития существующих компонентов информационной системы Компании;
- участие в проектировании систем информационной безопасности, их испытаниях и приемке в эксплуатацию;
- обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;
- контроль за предоставлением пользователям необходимых атрибутов доступа к ресурсам информационной системы Компании;

- наблюдение за функционированием системы защиты и ее элементов;
- организация проверок надежности функционирования системы защиты;
- регламентация и контроль за действиями администраторов и менеджеров ресурсов информационной системы Компании, связанных с информационной безопасностью Компании;
- контроль за соблюдением пользователями и обслуживающим персоналом установленных правил обращения с информацией;
- принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты.

Для решения задач, возложенных на подразделение информационной безопасности, его сотрудники должны иметь следующие права:

- определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в указанной области;
- получать информацию от пользователей информационной системы по любым аспектам применения информационных технологий в Компании;
- участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;
- участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;
- контролировать деятельность пользователей информационной системы по вопросам обеспечения информационной безопасности;
- получать доступ во все помещения, где установлены технические средства информационной системы Компании;
- санкционировать приостановку обработки информации при наличии и до устранения непосредственной угрозы для ее безопасности.

4.4.8. Ответственность за нарушения установленного порядка пользования ресурсами информационной системы Компании. Расследование/исследование нарушений

Любое грубое нарушение порядка и правил пользования информационными ресурсами Компании должно расследоваться. К виновным должны применяться адекватные законные меры воздействия. Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с информацией, должна определяться уровнем нанесенного ущерба, наличием злого умысла и другими факторами по усмотрению руководства Компании.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. закрепление за каждым пользователем персонального идентификатора, на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности, а также контроль за проведенными операциями в информационной системе Компании;
- проверка подлинности пользователей (аутентификация) на основе их идентификаторов, сертификатов, паролей, ключей, хранимых на различной физической основе, биометрических характеристик личности и т.п.;

- регистрация (протоколирование) доступа к компонентам и ресурсам информационной системы с указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимодействия и его результата;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

5. Средства обеспечения информационной безопасности

Для обеспечения информационной безопасности Компании используются следующие средства защиты:

- физические средства;
- технические средства;
- средства управления системой информационной безопасности;
- средства оценки эффективности систем защиты.

5.1. Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, 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 информационной системы может осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в них посторонних лиц, хищение документов и носителей информации, самих защищаемых средств, а также исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств съема (перехвата) информации.

5.2. Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности информации по всем направлениям защиты в состав системы защиты могут быть включены следующие средства:

- средства разграничения доступа к данным;
- средства криптографической защиты информации;
- средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;
- средства реагирования на нарушения режима информационной безопасности;
- средства снижения уровня и информативности побочных излучений, создаваемых компонентами информационной системы, предназначенными для обработки закрытой информации;
- средства маскировки от оптических средств наблюдения;
- средства активного зашумления в радио и акустическом диапазонах.

На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей;
- управление доступом пользователей в помещения, к физическим и информационным ресурсам;

- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;
- защита данных системы информационной безопасности от доступа всех пользователей, включая системных администраторов.

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

5.3. Средства управления системой информационной безопасности

Управление системой информационной безопасности представляет собой целенаправленное воздействие на компоненты системы информационной безопасности (организационные, технические, программные и криптографические) с целью достижения требуемого уровня защищенности циркулирующей в информационной системе Компании информации.

Главной целью организации управления системой информационной безопасности является обеспечение надежной защиты информации в процессе ее обработки, хранения и передачи.

Управление системой информационной безопасности может быть реализовано при помощи специализированной подсистемы, представляющей собой совокупность органов управления, технических, программных и криптографических средств, организационных мероприятий и взаимодействующих друг с другом пунктов управления различных уровней.

5.4. Средства контроля эффективности системы защиты

Контроль эффективности системы защиты информации осуществляется с целью своевременного выявления и предотвращения несанкционированного доступа к информационным и другим ресурсам, блокирования, искажения, разрушения или утечки информации, а также повреждения или уничтожения компонентов информационной системы Компании и самой системы защиты.

Контроль может проводиться как подразделением информационной безопасности Компании, так и привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

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

6. Техническая политика в области обеспечения безопасности информации

Реализация технической политики в области обеспечения безопасности информации должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информации не только с помощью одного отдельного средства (мероприятия), но и с помощью их простой совокупности. Необходимо их системное согласование между собой (комплексное применение), а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищенном исполнении при оптимальном соотношении технических (аппаратных, программных) средств и организационных мероприятий.

Основными направлениями реализации технической политики информационной безопасности Компании являются:

- обеспечение защиты ресурсов Компании от повреждения или уничтожения за счет несанкционированного доступа и специальных воздействий;
- обеспечение защиты информации от блокирования, утечки, разрушения или искажения при ее обработке, хранении и передаче по каналам связи.

Система информационной безопасности Компании должна предусматривать комплекс организационных, программных и технических средств и мер по защите информации в процессе ее обработки и хранения, при передаче информации по каналам связи, при ведении конфиденциальных переговоров, при использовании технических и программных средств.

В рамках указанных направлений технической политики информационной безопасности осуществляются:

- реализация разрешительной системы допуска пользователей и обслуживающего персонала к информационным и другим ресурсам;
- реализация системы инженерно-технических и организационных мер охраны, предусматривающей многорубежность и равнопрочность построения охраны (территории, здания, помещения) с комплексным применением современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;
- ограничение доступа к ресурсам, связанным с обработкой и хранением конфиденциальной информации, а также в здания и помещения, где проводятся работы конфиденциального характера;
- разграничение доступа пользователей и обслуживающего персонала к ресурсам Компании и компонентам системы защиты информации;
- учет информационных ресурсов, регистрация действий пользователей и обслуживающего персонала, контроль за доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;
- предотвращение внедрения в корпоративную информационную систему вредоносного программного обеспечения (вирусов, троянских коней, программных закладок и т.п.);
- реализация инфраструктуры открытого ключа, криптографическая защита конфиденциальной информации, передаваемой по открытым каналам связи;
- надежное хранение документов и носителей информации, ключей (ключевой документации) и их обращение, исключающее хищение, подмену и уничтожение;
- необходимое резервирование технических средств и дублирование массивов и носителей информации.

7. Формирование режима безопасности информации

С учетом выявленных угроз безопасности информации, режим защиты должен формироваться как совокупность способов и мер защиты циркулирующей в информационной среде Компании информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, влекущих за собой нанесение ущерба владельцам или пользователям информации.

Комплекс мер по формированию режима обеспечения безопасности информации включает:

- установление организационно-правового режима обеспечения безопасности информации (разработку необходимых нормативных документов, работа с персоналом, правил делопроизводства);
- выполнение организационно-технических мероприятий по защите конфиденциальной информации от утечки;

- организационные и программно-технические мероприятия по предупреждению несанкционированных действий с информационными ресурсами Компании;
- комплекс мероприятий по контролю функционирования информационной системы Компании после случайных или преднамеренных воздействий;
- комплекс оперативных мероприятий подразделения безопасности по предотвращению (выявлению) проникновения на территорию и в помещения лиц, имеющих отношение к криминальным структурам.

Организационно-правовой режим предусматривает создание и поддержание правовой базы безопасности информации, в частности, разработку и введение в действие следующих организационно-распорядительных документов:

- Положение о коммерческой тайне в Компании;
- Перечень сведений, составляющих служебную и коммерческую тайну;
- Положение по организации и ведению конфиденциального делопроизводства;
- Инструкции и функциональные обязанности сотрудников;
- Другие нормативные документы, входящие в состав Политики информационной безопасности.

Организационно-технические мероприятия по защите конфиденциальной информации от утечки предусматривают:

- комплекс мер и соответствующих технических средств, предотвращающих или ослабляющих утечку информации (пассивная защита);
- комплекс мер и соответствующих технических средств, создающих помехи при съеме информации – (активное противодействие);
- комплекс мер и соответствующих технических средств, позволяющих выявлять каналы утечки информации (поиск и обнаружение).

Физическая охрана компонентов информационной системы Компании включает:

- организацию системы охранно-пропускного режима и системы контроля допуска на объект;
- введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки конфиденциальной информации (кодовые и электронные замки, карточки допуска и т.д.);
- визуальный и технический контроль контролируемой зоны объекта защиты;
- применение систем охранной и пожарной сигнализации.

Выполнение режимных требований при работе с конфиденциальной информацией предполагает:

- разграничение допуска к ресурсам корпоративной информационной системы;
- ведение учета ознакомления сотрудников с конфиденциальной информацией;
- заключение с сотрудниками отдельного Соглашения о неразглашении ставшей им доступной конфиденциальной информации;
- организация уничтожения информационных отходов (бумажных, магнитных, оптических и т.д.);
- оборудование служебных помещений сейфами, шкафами для хранения носителей информации.

Мероприятия технического контроля предусматривают:

- контроль за проведением технического обслуживания, ремонта носителей информации и средств вычислительной техники;
- проверки поступающего оборудования, предназначенного для обработки конфиденциальной информации, на наличие специально внедренных закладных программ и устройств;

- оборудование компонентов информационной системы устройствами защиты от сбоев электропитания и помех в линиях связи;
- защита выделенных помещений при проведении закрытых работ (переговоров);
- постоянное обновление технических и программных средств защиты от несанкционированного доступа к информации в соответствие с меняющейся оперативной обстановкой.

8. История изменений

№	Дата	Версия	Предмет изменений	Автор
1.				
2.				
3.				