РОССИЙСКАЯ ФЕДЕРАЦИЯ
ХАНТЫ-МАНСИЙСКИЙ АВТОНОМНЫЙ ОКРУГ-ЮГРА
ГОРОД ОКРУЖНОГО ЗНАЧЕНИЯ СУРГУТ

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«МЕДИЦИНСКИЙ ЦЕНТР НАИРИ МЕД»
(ООО «МЦ НАИРИ МЕД»)

628407, Ханты-Мансийский Автономный Округ - Югра, г.о. Сургут, г. Сургут, ул. Семена Билецкого, д. 6, помещ. этаж 1
ОГРН 1228600003158, ИНН 8602306022, КПП 860201001

Утверждаю
Генеральный директор ООО «МЦ НАИРИ МЕД»
Т.О. Мнацаканян _____
«01» января 2026 года

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Рег.№ ЛНА-2

г. Сургут
2026 год

1. Назначение и область применения.

1.1. Настоящая политика информационной безопасности (далее – Политика) ООО «МЦ НАИРИ МЕД» (далее – Общество) определяет систему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется Общество в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в Обществе.

1.2. Область применения настоящей Политики распространяется на все структурные подразделения Общества.

2. Термины, определения, сокращения.

2.1. В настоящей Политике использованы следующие термины и определения:

Автоматизированная система – организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей потребителей информации.

Вредоносные программы – программы или измененные программы объекта информатизации, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нарушению работы.

Доступ к информации – ознакомление с информацией или получение возможности ее обработки. Доступ к информации регламентируется ее правовым режимом и должен сопровождаться строгим соблюдением его требований. Доступ к информации, осуществленный с нарушениями требований ее правового режима, рассматривается как несанкционированный доступ.

Доступ к ресурсу – получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом.

Доступность информации – важнейшее свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Защищаемое помещение – помещение для размещения технических средств защищенного объекта информатизации, а также помещение, предназначенное для проведения семинаров, совещаний, бесед и других мероприятий, в котором циркулирует конфиденциальная речевая информация.

Информационная система – организационно упорядоченная совокупность документов (массивов документов), независимо от формы их представления, места хранения, и информационных технологий, в том числе с использованием вычислительной техники и связи. Информационная система Общества включает в себя множество всех документов, существующих в Обществе.

Информационная среда – совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом отношений.

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информация ограниченного распространения – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о резуль-

татах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Контрагент – сторона гражданско-правового договора, взаимодействующая с Обществом в качестве поставщиков и потребителей информационных ресурсов Общества в том или ином качестве.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Границей контролируемой зоны могут являться:

- периметр охраняемой территории Общества;
- ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

В отдельных случаях на период обработки техническими средствами секретной информации (проведения закрытого мероприятия) контролируемая зона временно может устанавливаться большей, чем охраняемая территория предприятия. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Компьютерная система – информация в виде:

- записей в памяти компьютеров, на электронных устройствах, на машинных носителях (элементы, файлы, блоки, базы данных, микропрограммы, прикладные и системные программы, пакеты и библиотеки программ, микросхемы, программно-информационные комплексы и др.);
- сообщений, передаваемых по сетям передачи данных;
- программно-информационного продукта, являющегося результатом генерации новой или обработки исходной документированной информации, предоставляемого непосредственно на экранах дисплеев, на внешних носителях данных (магнитные диски, магнитные ленты, оптические диски, дискеты, твердотельные накопители, бумага для распечатки и т.п.) или через сети передачи данных.

Корпоративная информационная система – автоматизированная система обработки информации Общества.

Легальный пользователь – пользователь, допущенный к информационным ресурсам Общества (в том числе работник, отвечающий за обслуживание и администрирование компонентов корпоративной информационной системы).

Лицензия в области защиты информации – разрешение на право проведения тех или иных работ в области защиты информации.

Несанкционированное действие – действие субъекта в нарушение установленных в системе правил обработки информации.

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Объект защиты – информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Организационный контроль эффективности защиты информации – проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Пароль – служебное слово, известное узкому кругу лиц (одному лицу) и используемое

для ограничения доступа к информации, в помещение, на территорию.

Пользователь – субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

Система информационной безопасности – совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенного для обеспечения информационной безопасности Общества.

Физический канал утечки информации – неконтролируемый физический путь от источника информации за пределы Общества или круга лиц, обладающих охраняемыми сведениями, посредством которого возможно неправомерное (несанкционированное) овладение нарушителем защищаемой информацией.

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

2.2. В настоящей Политике использованы следующие сокращения:

УБ – управление безопасности ООО «МЦ НАИРИ МЕД»;

ОВСУПП – отдел по внедрению систем управления производственными процессами.

3. Общие положения.

3.1. Объекты защиты

3.1.1. Основными объектами защиты системы информационной безопасности в Обществе являются:

- информационные ресурсы с ограниченным доступом, составляющие коммерческую тайну, персональные данные или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открытая (общедоступная) информация, необходимая для работы Общества, независимо от формы и вида ее представления;
- процессы обработки информации в информационной системе Общества информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные элементы информационной среды Общества;
- структура, состав и размещение основных объектов защиты, информационные связи.

3.1.2. К основным особенностям информационной среды Общества относятся:

- широкая территориальная распределенность компонентов информационной системы;
- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;
- значительное расширение сферы использования автоматизированных систем обработки информации, широкое многообразие и повсеместное распространение информационно-управляющих систем в Обществе;
- объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;
- абстрагирование владельцев данных от физических структур и места размещения данных (информации);
- наличие большого числа информационных каналов взаимодействия с «внешним миром» (источниками и потребителями информации);

- необходимость обеспечения непрерывности функционирования Общества;

- высокая интенсивность информационных потоков.

Защите подлежит вся информация и информационные ресурсы Общества, независимо от ее представления и местонахождения в информационной среде Общества:

- сведения, составляющие коммерческую тайну;

- сведения о частной жизни граждан (персональные данные), доступ к которым ограничен в соответствии с ФЗ «О персональных данных» и ФЗ «Об информации, информационных технологиях и о защите информации»;

- открытая информация, необходимая для обеспечения нормального функционирования Общества.

3.1.3. Все принадлежащие Обществу (в том числе на праве интеллектуальной собственности) информационно-технические ресурсы, включая компьютерное, телекоммуникационное и периферийное оборудование, электронную и голосовую почту, мобильные устройства и носители информации предоставляются для пользования работниками Общества исключительно в служебных целях и не предназначены для ведения конфиденциальной частной переписки, переговоров и/или хранения личной конфиденциальной информации. Вся электронная переписка, сгенерированная (созданная, полученная) работниками Общества посредством технических средств, информационных систем, каналов связи или передачи данных, принадлежащих Обществу, является собственностью Общества.

3.1.4. В целях контроля за деятельностью работников Общества на рабочем месте и защиты от утечки информации по техническим каналам связи Общество оставляет за собой право без предварительного предупреждения:

- осуществлять запись, обработку и хранение информации о телефонных и иных переговорах, иных разговоров;

- внедрять специализированное программное и аппаратное обеспечение для проверки и мониторинга использования компьютерных систем;

- проверить состояние компьютерных систем, а также информацию, которая в них содержится;

- отслеживать, изучать, удалять или изменять любые электронные сообщения, которые проходят через корпоративную систему электронной почты или системы мгновенного обмена сообщениями.

3.2. Цели и задачи обеспечения безопасности информации

3.2.1. Субъектами информационных отношений при обеспечении информационной безопасности Общества являются:

- Общество, как собственник информационных ресурсов;

- подразделения Общества, участвующие в информационном обмене;

- руководство и работники структурных подразделений Общества в соответствии с возложенными на них функциями;

- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационной системе Общества;

- другие юридические и физические лица, задействованные в обеспечении выполнения Обществом своих функций (консультанты, разработчики, обслуживающий персонал, организации, привлекаемые для оказания услуг и пр.).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимой им информации (ее доступности);

- достоверности (полноты, точности, адекватности, целостности) информации;

- конфиденциальности (сохранения в тайне) определенной части информации;

- защиты от навязывания им ложной (недостоверной, искаженной) информации;

- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с информацией;

- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации.

3.2.2. Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Общества от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация уровня операционного и других рисков (риск нанесения урона деловой репутации Общества, правовой риск и т.д.).

3.2.3. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации для легальных пользователей (устойчивого функционирования информационной системы Общества, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в информационной системе Общества и передаваемой по каналам связи;
- конфиденциальности – сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи.

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

3.2.4. Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности Общества 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 Общества;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого неправомерными действиями физических и юридических лиц ущерба, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационной системы Общества посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Общества (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);
- защита от несанкционированной модификации используемых в корпоративной информационной системе Общества программных средств, а также защита информационной системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки при ее обработке, хранении и передаче по каналам связи.

3.2.5. Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов информационной системы Общества (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- журналированием (хронологической записью) действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;

- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Общества, по вопросам обеспечения безопасности информации;

- подготовкой работников, ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

- наделением каждого работника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Общества;

- четким знанием и строгим соблюдением всеми пользователями информационной системы Общества требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- персональной ответственностью за свои действия каждого работника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Общества;

- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Общества;

- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

- эффективным контролем за соблюдением пользователями информационных ресурсов Общества требований по обеспечению безопасности информации;

- внедрением специализированного программного и аппаратного обеспечения для проверки и мониторинга использования информационных систем;

- юридической защитой интересов Общества при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий как со стороны этих организаций, так и от несанкционированных действий третьих лиц.

4. Обеспечение информационной безопасности.

4.1. Угрозы безопасности информации и их источники

4.1.1. Все множество потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;

Искусственные угрозы – угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п.;

- преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

4.1.2. Основными источниками угроз безопасности информации Общества являются:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационной системы Общества (в том числе работников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере чувствительной информации или нарушению работоспособности компонентов информационной системы;

- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым

умыслом и т.п.) действия легально допущенных к информационным ресурсам Общества пользователей (в том числе работников, 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 Общества;

- удаленное несанкционированное вмешательство посторонних лиц из территориально удаленных сегментов корпоративной информационной системы и внешних сетей общего назначения (прежде всего сеть 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 Общества 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.

4.2. Выполнение задач и функций по обеспечению информационной безопасности УБ осуществляет во взаимодействии с ОВСУПП.

4.2.1. На УБ возлагается решение следующих основных задач:

- проведение в жизнь политики обеспечения безопасности информации, определение требований к системе защиты информации;

- анализ текущего состояния обеспечения безопасности информации;

- организация мероприятий и координация работ всех подразделений Общества по комплексной защите информации;

- контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

4.2.2. Основные функции УБ по обеспечению информационной безопасности заключаются в следующем:

- формирование требований к системам защиты в процессе создания и дальнейшего развития существующих компонентов информационной системы Общества;

- участие в проектировании систем защиты, их испытаниях и приемке в эксплуатацию;

- обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;

- наблюдение за функционированием системы защиты и ее элементов;

- проверка надежности функционирования системы защиты;

- разработка мер нейтрализации моделей возможных атак;

- обучение пользователей и обслуживающего персонала информационных систем правилам безопасной обработки информации;

- оказание методической помощи работникам Общества в вопросах обеспечения информационной безопасности;

- контроль за действиями администраторов баз данных, серверов и сетевых устройств;

- контроль за соблюдением пользователями и обслуживающим персоналом информационных систем установленных правил обращения с информацией;

- организация по указанию руководства служебных расследований по фактам нарушения правил обращения с информацией и оборудованием;

- принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;

- сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности.

4.3. Ответственность за нарушения установленного порядка пользования ресурсами информационной системы Общества

Работники общества несут юридическую ответственность за нарушение правил работы

с информацией в порядке, предусмотренном законодательством Российской Федерации.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора, на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;
- проверка подлинности пользователей (аутентификация) на основе паролей, ключей на различной физической основе, биометрических характеристик личности и т.п.;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

4.4. Средства обеспечения информационной безопасности Общества

Для обеспечения информационной безопасности Общества могут использоваться следующие средства защиты:

- физические средства;
- технические средства;
- средства идентификации и аутентификации пользователей;
- средства разграничения доступа;
- средства обеспечения и контроля целостности;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства.

Средства защиты должны применяться ко всем чувствительным ресурсам информационной системы Общества, независимо от их вида и формы представления информации в них.

4.4.1. Физическая защита зданий, помещений, объектов и средств информатизации должна организовываться УБ и 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 средств информатизации, а также исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств съема информации.

Для обеспечения физической безопасности компонентов информационной системы Общества необходимо осуществлять ряд организационных и технических мероприятий, включающих проверку оборудования, предназначенного для обработки конфиденциальной информации.

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

- средства разграничения доступа к данным;
- 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 Общества, предназначенными для обработки закрытой информации;
- средства криптографической защиты информации.

4.4.3. На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств;
- регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких

уровней регистрации;

- защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информацией, находящейся на нем.

4.4.4. С целью предотвращения работы с ресурсами информационной системы Общества посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

- путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);
- путем проверки знания ими паролей;
- путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

4.4.5. Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации информации должен обеспечиваться:

- средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);
- средствами электронной подписи, средствами учета;
- средствами подсчета контрольных сумм (для используемого программного обеспечения).

4.4.6. Средства оперативного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток несанкционированного доступа и т.п.), которые могут повлечь за собой нарушение Политики информационной безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов);
- получения твердой копии (печати) журнала регистрации событий безопасности;
- упорядочения журналов, а также установления ограничений на срок их хранения;
- оперативного оповещения УБ о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

- дата и время события;
- идентификатор субъекта, осуществляющего регистрируемое действие;
- действие (тип доступа).

4.5. Контроль эффективности системы защиты

Контроль эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

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

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия требованиям, установленным настоящей Политикой и иными локальными нормативными документами Общества.

Основными направлениями реализации технической концепции обеспечения безопасности информации Общества являются:

- обеспечение защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий;

- обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и при передаче по каналам связи.

Система обеспечения безопасности информации Общества 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, раскрывающих сведения с ограниченным доступом, при использовании технических и программных средств.

В рамках указанных направлений технической концепции обеспечения безопасности информации осуществляются:

- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации; 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 в здания и помещения, где проводятся работы конфиденциального характера и размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация, а также непосредственно к самим средствам информатизации и коммуникациям;

- разграничение доступа пользователей и обслуживающего персонала информационных систем к информационным ресурсам, программным средствам обработки (передачи) и защита информации в информационной системе Общества;

- учет документов, информационных массивов, регистрация действий пользователей и обслуживающего персонала информационных систем, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;

- предотвращение внедрения в корпоративную информационную систему Общества программ-вирусов, программных закладок;

- реализация инфраструктуры с открытым ключом, криптографическая защита информации ограниченного пользования, обрабатываемой и передаваемой средствами вычислительной техники по открытым каналам связи;

- надежное хранение документов и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее хищение, подмену и уничтожение;

- необходимое резервирование технических средств и дублирование массивов и носителей информации;

- обеспечение акустической защиты помещений, в которых обсуждается информация конфиденциального характера;

- противодействие оптическим и лазерным средствам наблюдения.

4.6. Формирование режима безопасности информации

4.6.1. С учетом выявленных угроз безопасности информации Общества режим защиты

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

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

- положение о режиме коммерческой тайны, которое регламентирует организацию, порядок работы со сведениями, составляющими коммерческую тайну Общества, обязанности и ответственность работников, допущенных к этим сведениям, порядок передачи материалов, содержащих сведения, составляющим коммерческую тайну Общества, государственным (коммерческим) учреждениям и организациям;
- перечень сведений, составляющих конфиденциальную информацию Общества, который определяет сведения, отнесенные к категориям конфиденциальных, уровень и сроки обеспечения ограничений по доступу к защищаемой информации;
- приказы и распоряжения по установлению режима безопасности информации (о допуске работников к конфиденциальной информации, о назначении администраторов и лиц, ответственных за работу с конфиденциальной информацией в корпоративной информационной системе и т.п.);
- инструкции и функциональные обязанности работников (по организации охранно-пропускного режима, по организации делопроизводства, по администрированию информационных ресурсов корпоративной информационной системы);
- другие нормативные документы.

4.6.3. Организационно-технические мероприятия по защите информации ограниченного распространения от утечки по техническим каналам предусматривают:

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

4.6.4. Физическая охрана объектов информатизации (компонентов Информационной системы Общества) включает:

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

4.6.5. Выполнение режимных требований при работе с конфиденциальной информацией предполагает:

- разграничение допуска к информационным ресурсам ограниченного пользования;
- разграничение допуска к ресурсам корпоративной информационной системы;
- ведение учета ознакомления работников с информацией ограниченного пользования;
- включение в функциональные обязанности работников обязательства о неразглашении и сохранности сведений ограниченного пользования;
- организация уничтожения конфиденциальной информации (бумажных, магнитных носителей и т.д.);
- оборудование служебных помещений сейфами, шкафами для хранения бумажных и магнитных носителей информации.

5. Ответственность.

5.1. Ответственность за выполнение требований настоящей Политики возлагается на работников Общества.

5.2. Ответственность за контроль соблюдения требований настоящей Политики возлагается на УБ.

5.3. Ответственность контрагента за соблюдение требований настоящей Политики устанавливается в соответствии с условиями заключенного между Обществом и контрагентом Соглашения о конфиденциальности и договора.

6. Нормативные ссылки.

Настоящее Положение разработано на основании и с использованием ссылок на:

6.1. Законодательство и иные нормативно-правовые акты Российской Федерации:

6.1.1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6.1.2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».