Утверждено

Приказом ООО «My Company»

от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2024г.

**Политика информационной безопасности**

**ООО «My Company»**

г. Москва

2024г

**Содержание**

[1 Термины, определения и сокращения 4](#_Toc170461573)

[2 Нормативные ссылки 5](#_Toc170461574)

[3 Общие положения 6](#_Toc170461575)

[3.1 Цели обеспечения ИБ 6](#_Toc170461576)

[3.2 Основные задачи обеспечения ИБ 7](#_Toc170461577)

[3.3 Основные принципы обеспечения ИБ 7](#_Toc170461578)

[3.4 Направления обеспечения ИБ 8](#_Toc170461579)

[4 Распределение обязанностей н ответственности по обеспечению ИБ 8](#_Toc170461580)

[4.1.1 Специалист по защите информации 9](#_Toc170461581)

[4.1.2 Владельцы информационных активов систем обработки информации 9](#_Toc170461582)

[4.1.3 Системные администраторы 9](#_Toc170461583)

[4.1.4 Администраторы ИБ 10](#_Toc170461584)

[4.1.5 Администраторы автоматизированных рабочих мест 11](#_Toc170461585)

[4.1.6 Администраторы средств защиты информации 11](#_Toc170461586)

[4.1.7 Руководители структурных подразделений 12](#_Toc170461587)

[4.1.8 Работники, ответственные за информационную безопасность в структурных подразделениях Общества 12](#_Toc170461588)

[4.1.9 Работники Общества 12](#_Toc170461589)

[5 Документы по защите информации 13](#_Toc170461590)

[6 Процессы обеспечения ИБ 13](#_Toc170461591)

[6.1 Обеспечение ИБ на этапах жизненного цикла объектов информационной инфраструктуры 14](#_Toc170461592)

[6.2 Обеспечение ИБ при эксплуатации систем обработки информации и использовании информационных активов 15](#_Toc170461593)

[6.2.1 Физическая защита объектов информационной инфраструктуры Общества 15](#_Toc170461594)

[6.2.2 Защита территорий, зданий и помещений Общества 16](#_Toc170461595)

[6.2.3 Организация безопасной эксплуатации средств обработки, хранения и передачи информации 16](#_Toc170461596)

[6.2.4 Защита от вредоносного программного обеспечения 16](#_Toc170461597)

[6.2.5 Резервирование информационных активов и технических средств обработки, хранения и передачи информации 17](#_Toc170461598)

[6.2.6 Обеспечение сетевой безопасности 18](#_Toc170461599)

[6.2.7 Обеспечение ИБ при взаимодействии с сетью Интернет 19](#_Toc170461600)

[6.2.8 Обеспечение ИБ при использовании съемных носителей информации, мобильных и коммуникационных устройств 20](#_Toc170461601)

[6.2.9 Защита ПО 21](#_Toc170461602)

[6.2.10 Регистрация и учет событий ИБ 22](#_Toc170461603)

[6.2.11 Криптографическая защита информации 22](#_Toc170461604)

[6.3 Контроль доступа 22](#_Toc170461605)

[6.3.1 Управление доступом пользователей 22](#_Toc170461606)

[6.3.2 Ответственность пользователей при доступе к информационным ресурсам 23](#_Toc170461607)

[6.4 Контроль защищенности 23](#_Toc170461608)

[6.5 Обеспечение соответствия требованиям по ИБ 24](#_Toc170461609)

[6.5.1 Обеспечение режима коммерческой тайны 24](#_Toc170461610)

[6.5.2 Обеспечение защиты персональных данных 24](#_Toc170461611)

[6.5.3 Организация работы с персоналом по вопросам ИБ 24](#_Toc170461612)

[6.5.4 Обеспечение ИБ при работе с контрагентами 25](#_Toc170461613)

[6.6 Предотвращение утечки защищаемой информации по техническим каналам 26](#_Toc170461614)

[7 Ответственность руководства и работников Общества 27](#_Toc170461615)

[8 Порядок пересмотра Политики 27](#_Toc170461616)

# Термины, определения и сокращения

В настоящей Политике информационной безопасности применены основные термины и определения», а также следующие сокращения и определения:

**BIOS** - Basic Input/Output System (базовая система ввода-вывода);

**UEFI** - Unified Extensible Firmware Interface (унифицированный расширяемый интерфейс прошивки);

**АРМ** - автоматизированное рабочее место;

**ИС** - информационная система;

**ЛВС** - локальная вычислительная сеть;

**ОС** - операционная система;

**ПО** - программное обеспечение;

**СЗИ** - система защиты информации (СЗИ).

**Автоматизированное рабочее место (АРМ)** - комплекс программноаппаратных средств (например, персональный компьютер с набором программного обеспечения и подключенными периферийными устройствами), предназначенный для выполнения определенных производственных задач.

**Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Информационная безопасность (ИБ)** - состояние защищенности интересов ООО «My Company» в условиях угроз в информационной сфере. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих обработку информации, а также системы регулирования возникающих при этом отношений. Информационная безопасность достигается определением, достижением и поддержанием конфиденциальности, целостности, доступности и достоверности информации, принадлежащий или обрабатываемой ООО «My Company», а также обеспечением аутентичности, неотказусмости и подотчетности участников процесса обработки такой информации.

**Информационная инфраструктура** - совокупность программнотехнических средств и вычислительных сетей, обеспечивающих предоставление информационных активов и услуг, необходимых для выполнения бизнес-процессов ООО «My Company».

**Конфиденциальная информация** - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

**Направление обеспечения информационной безопасности** - укрупненная часть деятельности ООО «My Company» по обеспечению информационной безопасности, состоящая из одного или нескольких процессов обеспечения информационной безопасности.

**Обработка информации** - любое действие, совершаемое с информацией, включая получение, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование (ознакомление), передачу (распространение, предоставление, доступ), блокирование, удаление.

**Общество** - ООО «My Company», его филиалы и обособленные структурные подразделения.

**Объект защиты (ОЗ)** - информационные активы, технические и программные средства их обработки, передачи, хранения (системы обработки информации).

**Контроль состояния ИБ** - деятельность, связанная с определением способности процессов обеспечения информационной безопасности поддерживать достижение целей информационной безопасности.

**Процесс обеспечения информационной безопасности** - совокупность процедур, выполняемых работниками разных подразделений, приводящая к получению законченного и значимого результата по определенному направлению обеспечения информационной безопасности.

**Сетевое оборудование** - совокупность технических и программных средств обеспечивающих объединение систем обработки информации в вычислительные сети, функционирование и защиту таких сетей (коммутаторы, маршрутизаторы, межсетевые экраны, системы обнаружения и предотвращения вторжений и т.д.).

**Система обработки информации** - совокупность технических средств, программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации. В контексте данной Политики к системам обработки информации отнесены все объекты защиты, с помощью которых происходит обработка информации (серверы, информационно-управляющие системы, автоматизированные системы управления, системы связи и передачи данных, прочие системы).

**Система обеспечения информационной безопасности (СОИБ)** - часть общей системы управления организации, основанная на принципах формирования требований к объектам защиты на основании принятых норм и правил в ООО «My Company».

**Системно-техническая инфраструктура** - совокупность аппаратно-программных средств, предназначенных для обеспечения надежного и бесперебойного функционирования отдельных информационных систем и инфраструктурных служб.

**Структурное подразделение (ООО «My Company»)** - подразделение, предусмотренное организационной структурой ООО «My Company» и находящееся в непосредственном подчинении генерального директора, соответствующего заместителя генерального директора или другого менеджера компании. К структурным подразделениям относятся: управления, самостоятельные отделы и службы, бухгалтерия ООО «My Company».

**Требование по информационной безопасности** - установленное нормативными правовыми актами правило (или норма), которое должно быть выполнено при организации и осуществлении обеспечения информационной безопасности, или допустимое значение показателя защищенности безопасности информации.

# Нормативные ссылки

Гражданский кодекс Российской Федерации.

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

Федеральный закон № 98-ФЗ «О коммерческой тайне».

Федеральный закон № 184-ФЗ «О техническом регулировании».

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

Федеральный закон № 63-ФЗ «Об электронной подписи».

Положение о конфиденциальной информации (коммерческой тайны) в ООО «My Company», утвержденное приказом ООО «My Company» от 01.12.2013 № 1/011213.

Политика защиты и обработки персональных данных работников ООО «My Company», утвержденное приказом Общества от 01.09.2022 № 1/01-09/2022.

# Общие положения

Настоящая Политика является нормативным документом верхнего уровня в области обеспечения ИБ ООО «My Company» (далее - Общество).

Настоящая Политика представляет собой официально принятую систему взглядов руководства Общества на цели, задачи, основные принципы и направления деятельности в области обеспечения ИБ Общества.

В рамках Политики руководство Общества заявляет, что:

- информационные активы и технологии играют важную роль в достижении бизнес-целей Общества;

- информация является ценным активом, требующим защиты независимо от форм ее представления;

- в своей деятельности Общество сталкивается с широким спектром угроз ИБ, как внутреннего, так и внешнего характера, реализация которых может привести к ущербу (финансовые потери, юридическая ответственность, репутационные потери, дезорганизация и т.д);

- стратегической целью Общества в области ИБ является снижение рисков, связанных с нарушением безопасности информации, до приемлемого к принятию уровня, при котором обеспечивается непрерывность и эффективность бизнес-процессов, соблюдение взятых на себя обязательств перед контрагентами и устойчивое функционирование Общества в целом;

- стратегической задачей Общества в области ИБ является поддержание требуемого уровня защищенности информации в процессах ее получения, обработки, хранении и передачи.

Настоящая Политика разработана с учетом требований законодательных актов Российской Федерации, приведенных в разделе 2.

Положения настоящей Политики являются основой для разработки организационно-распорядительных, нормативных и методических документов, регламентирующих порядок обеспечения И Б в Обществе, с учетом современного состояния, целей, задач и правовых основ процессов получения, обработки, хранения и передачи информации.

Положения настоящей Политики распространяются на Общество в целом и являются обязательными к применению всеми работниками Общества.

Функции по обеспечению ИБ, отнесенные настоящей Политикой к компетенции структурных подразделений Общества, филиалов и обособленных структурных подразделений возлагаются на работников подразделений в соответствии со штатным расписанием или организационно-распорядительными документами Общества.

## Цели обеспечения ИБ

Основными целями обеспечения ИБ Общества являются:

* предотвращение или существенное уменьшение возможности нанесения ущерба жизненно важным интересам Общества вследствие реализации актуальных угроз ИБ;
* обеспечение безопасности, принадлежащей Обществу или обрабатываемой на законных основаниях конфиденциальной информации;
* правовая защита информации;
* недопущение деструктивного воздействия на элементы информационной инфраструктуры Общества;
* обеспечение устойчивого функционирования информационной инфраструктуры Общества
* обеспечение законности при обработке защищаемой информации.

Основными целями настоящей Политики являются:

* создание методологической основы для формирования документов по защите информации в Обществе;
* установление форм участия структурных подразделений и работников Общества в процессе обеспечения ИБ.

## Основные задачи обеспечения ИБ

Обеспечение ИБ Общества достигается выполнением следующих основных задач:

* созданием организационных структур, обеспечивающих функционирование СОИБ;
* распределением обязанностей и ответственности за функционирование процессов СОИБ;
* разработкой и поддержанием в актуальном состоянии системы документов по защите информации;
* внедрением и поддержанием процессов обеспечения ИБ;
* реализацией организационных и технических мероприятий по обеспечению ИБ;
* установлением режима коммерческой тайны;
* созданием системы защиты персональных данных;
* контролем выполнения требований по ИБ, контролем эффективности применяемых мер защиты информации и совершенствованием СОИБ.

## Основные принципы обеспечения ИБ

Обеспечение ИБ Общества основывается на соблюдении следующих основных принципов:

* соблюдение требований законодательства Российской Федерации в области ИБ, нормативных документов федеральных органов исполнительной власти, уполномоченных в сфере обеспечения ИБ;
* планирование мероприятий по обеспечению ИБ;
* применение системных и комплексных решений при обеспечении ИБ;
* использование технических и программных средств, а также информационных активов, принадлежащих Обществу, только в производственных целях;
* наделение работников Общества минимально необходимыми правами на доступ к информационным ресурсам для выполнения ими своих должностных обязанностей;
* сегментированием информационной инфраструктуры по определяемым критериям;
* установление персональной ответственности должностных лиц за обеспечение выполнения требований по ИБ;
* приоритетное использование отечественных информационных и коммуникационных технологий, технических и программных средств;
* приоритетное использование в составе информационных систем ИО, встроенные функции которого обеспечивают выполнение установленных для указанных информационных систем требований по ИБ;
* совершенствование СОИБ на основе результатов расследования инцидентов ИБ, контроля соблюдения требований по ИБ и оценки эффективности принимаемых мер защиты информации.

Обеспечение ИБ при выполнении работ по эксплуатации/сопровождению автоматизированных, информационных или телекоммуникационных систем Общества в соответствии с требованиями нормативных и распорядительных документов Общества в области ИБ.

## Направления обеспечения ИБ

Общество, как обладатель самостоятельно разработанной и полученной на законных основаниях информации, устанавливает и регламентирует порядок обращения с такой информацией, включающий правовые, организационные и технические меры по ее защите.

Особое внимание уделяется регламентации мер по защите информации, ограничение доступа к которой предусматривается законодательством Российской Федерации, включая информацию, составляющую коммерческую тайну, и иную конфиденциальную информацию Общества.

Обеспечение ИБ в Обществе осуществляется по следующим основным направлениям:

* обеспечение ИБ при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов;
* обеспечение соответствия требованиям законодательства Российской Федерации в области ИБ, нормативных документов федеральных органов исполнительной власти, уполномоченных в сфере обеспечения ИБ;
* обеспечение режима коммерческой тайны;
* защита персональных данных;
* обеспечение ИБ при работе с внешними организациями;
* организация работы с персоналом по вопросам ИБ;
* управление инцидентами ИБ;
* формирование требований к программным и аппаратным средствам, используемым для защиты объектов информационной инфраструктуры;
* определение правового статуса и ответственности за нарушение установленных требований по ИБ всех субъектов информационных процессов Общества.

Данные направления реализуются в рамках соответствующих процессов обеспечения ИБ за счет принятия организационных и технических мер.

# Распределение обязанностей н ответственности по обеспечению ИБ

Организацию и обеспечение управления ИБ в Обществе осуществляет генеральный директор Общества.

Координацию деятельности по реализации настоящей Политики осуществляет специалист по информационной безопасности.

Непосредственно мероприятия по обеспечению ИБ организуют и проводят руководители структурных подразделений Общества. Руководители структурных подразделений Общества несут ответственность за состояние информационной безопасности в подразделениях.

Руководство Общества постоянно поддерживает необходимый уровень ИБ путем внедрения системы обеспечения ИБ, а также распределения обязанностей и ответственности работников Общества за ее внедрение, функционирование и совершенствование.

В Обществе разрабатывается и поддерживается в актуальном состоянии нормативная база системы обеспечения ИБ. осуществляется текущий и плановый (периодический) контроль выполнения требований ИБ при работе с информацией и средствами ее автоматизированной обработки.

С учетом особенностей конкретных объектов информационной инфраструктуры Общества в их отношении осуществляется:

* наделение необходимым уровнем полномочий работников Общества в отношении защищаемых информационных ресурсов;
* администрирование встроенных механизмов безопасности системного и прикладного программного обеспечения;
* администрирование дополнительно применяемых средств защиты информации;
* контроль выполнения работниками Общества требований в области ИБ;
* контроль функционирования средств защиты информации и механизмов обеспечения безопасности.

Конкретные задачи (обязанности) и функции по обеспечению ИБ структурных подразделений и должностных лиц Общества, устанавливаются нормативными документами Общества по обеспечению ИБ, положениями о структурных подразделениях и должностными инструкциями работников.

### Специалист по защите информации

Функции специалиста по защите информации определены и утверждены генеральным директором Общества, основными из которых являются:

* планирование работ по ИБ:
* формирование и поддержание в актуальном состоянии системы документов по обеспечению ИБ в Обществе:
* организация и контроль выполнения работ по обеспечению защиты информации, составляющей коммерческую тайну, и иной конфиденциальной информации в Обществе;
* координация деятельности структурных подразделений и работников Общества по обеспечению ИБ;
* контроль реализации и эффективности мер обеспечения ИБ в Обществе, в том числе при эксплуатации средств обработки, хранения и передачи информации, и внесение рекомендаций по их совершенствованию;
* организация управления инцидентами ИБ в Обществе.

### Владельцы информационных активов систем обработки информации

Для каждой системы обработки информации (объекта информационной инфраструктуры, в том числе автоматизированной, информационно-управляющей и иной информационной системы) должны быть определены структурные подразделения - владельцы информационных активов. Владельцы информационных активов организуют работы по созданию системы обработки информации, а также систем защиты информации в составе системы обработки информации.

Основные обязанности Владельцев информационных активов систем обработки информации:

* определение наличия информации ограниченного доступа в информационных активах, обрабатываемых в системах обработки информации;
* классификация систем обработки информации по требованиям безопасности информации в установленном порядке;
* организация работ на всех стадиях жизненного цикла систем обработки информации;
* утверждение документов на систему защиты информации систем обработки информации.

Для систем обработки информации Общества, Владельцами информационных активов систем обработки информации назначаются структурные подразделения Общества, которые являются основными пользователями.

### Системные администраторы

За каждой системой обработки информации (сервером, автоматизированной системой управления, информационной/информационно-управляющей системой, сервисом, программно-аппаратным комплексом, активным сетевым оборудованием и т.п.) или составной частью системы обработки информации (объектом защиты) должен быть назначен локальным нормативным актом Общества (приказом, распоряжением, должностной инструкцией) соответствующий администратор (системный администратор, сетевой администратор, администратор прикладного ПО, администратор системы управления базами данных и т.п.).

4.1.4 Системные администраторы или входящего в состав такой системы объекта защиты назначаются работники структурных подразделений Общества, обеспечивающих сопровождение эксплуатации систем обработки информации.

Основными задачами администраторов систем обработки информации являются:

* организация и проведение резервного копирования информационных ресурсов средств обработки информации;
* обеспечение доступности системы обработки информации и целостности обрабатываемых в ней информационных активов;
* обеспечение безотказной работы и восстановление работоспособности систем обработки информации (элементов систем) при возникновении нештатной ситуации;
* мониторинг событий системы обработки информации;
* информирование службы ИБ или администратора ИБ о выявленных инцидентах ИБ или подозрениях на инцидент;

Также, в рамках своей компетенции, администраторы систем обработки информации решают следующие задачи:

* администрирование встроенных механизмов безопасности средств обработки, хранения и передачи информации в системах;
* обеспечение соответствия заданных настроек механизмов безопасности, а также задач и процессов их обеспечивающих;
* управление доступом и полномочиями пользователей, в том числе прекращение доступа по установленным основаниям;
* обеспечение функционирования процессов обеспечения ИБ;
* ведение и поддержание в актуальном состоянии документации на систему обработки информации, в том числе параметров настроек безопасности.

Перечень конкретных работ по обеспечению ИБ систем обработки информации определяются локальными нормативными документами Общества по ИБ.

### Администраторы ИБ

В Обществе организуется администрирование ИБ, направленное на контроль выполнения установленных требований по ИБ, контроль правил доступа к объектам информационной инфраструктуры, порядка обращения с защищаемой информацией при ее обработке, хранении и передаче.

Администрирование ИБ включает:

* контроль соответствия заданных настроек встроенных механизмов безопасности средств обработки, хранения и передачи информации, средств и систем защиты информации, эксплуатационной документации;
* контроль соответствия предоставленных пользователям прав доступа к информационным ресурсам;
* аудит событий систем обработки информации (анализ журнала учета событий, регистрируемых средствами защиты, операционными системами и т.д.) с целью выявления возможных нарушений установленных требований по обеспечению ИБ или инцидентов ИБ;
* первичное реагирование на выявленные инциденты ИБ;
* информирование руководства Общества о выявленных нарушениях требований по ИБ и инцидентах ИБ.

Для объектов информационной инфраструктуры Общества, для которых в установленном порядке предъявляются требования по обработке информации, составляющей коммерческую тайну, и иной конфиденциальной информации Общества - администраторы ИБ назначаются из числа работников ИТ и/или ИБ.

На администраторов ИБ возлагаются обязанности по контролю соответствия мер и средств защиты информации, применяемых в рамках объекта защиты, требованиям эксплуатационной документации и нормативных документов Общества в области ИБ.

Перечень конкретных работ по обеспечению ИБ определяются локальными нормативными документами Общества по ИБ.

### Администраторы автоматизированных рабочих мест

В Обществе должны быть определены ответственные за администрирование АРМ.

Администраторами АРМ назначаются работники структурных подразделений Общества, ответственных за системно-техническое обслуживание АРМ и сервисную ИТ-поддержку пользователей.

Основными задачами администраторов АРМ являются:

* сбор информации об АРМ, используемых в Обществе, включающей в том числе сведения о конфигурации, назначении, расположении и ответственном пользователе АРМ;
* системно-техническое обслуживание АРМ;
* обеспечение соответствия настроек АРМ, установленным в Обществе требованиям;
* установка, настройка и обновление системного, прикладного ПО, разрешенного к использованию в Обществе;
* установка и настройка периферийного оборудования в составе АРМ;
* техническая поддержка и консультирование пользователей по вопросам безопасной эксплуатации АРМ.

Перечень конкретных работ по обеспечению ИБ АРМ определяются локальными нормативными документами Общества по ИБ.

### Администраторы средств защиты информации

В Обществе должны быть определены ответственные за настройку встроенных механизмов безопасности средств обработки, хранения и передачи информации, а также администрирование средств и систем защиты информации.

Администраторами СЗИ назначаются работники структурных подразделений Общества, ответственных за обеспечение работоспособности таких средств.

Основными задачами администраторов СЗИ являются:

* непосредственное управление СЗИ в целях обеспечения их устойчивого и безопасного функционирования;
* поддержание в работоспособном состоянии и обеспечение соответствия настроек СЗИ эксплуатационной документации;
* обеспечение выполнения СЗИ функций защиты информации в отношении всех объектов защиты, к которым применяется СЗИ;
* обеспечение безотказной работы и восстановление работоспособности СЗИ при возникновении нештатной ситуации;
* управление доступом и полномочиями пользователей СЗИ. в том числе прекращение доступа по установленным основаниям;
* периодический контроль журналов событий, генерируемых СЗИ;
* информирование руководства Общества или администратора ИБ о выявленных инцидентах ИБ или подозрениях на инцидент;
* подготовка систематизированных данных, полученных в процессе работы СЗИ, для использования в процедурах реагирования на инциденты ИБ.

Перечень конкретных работ по обеспечению ИБ СЗИ определяются локальными нормативными документами Общества по ИБ.

### Руководители структурных подразделений

Ответственность за выполнение требований ИБ работниками структурного подразделения Общества возлагается на руководителя структурного подразделения.

Руководитель структурного подразделения Общества отвечает за:

* доведение до работников структурного подразделения Общества нормативных актов и методических документов, регламентирующих вопросы обеспечения ИБ;
* контроль выполнения работниками требований по ИБ и возложенных на них задач в рамках функционирования процессов обеспечения И Б;
* организацию допуска работников подразделения к информационным активам и системам обработки информации Общества;
* согласование допуска работников других подразделений и организаций к информационным активам и системам обработки своего подразделения;
* организацию заключения соглашений о конфиденциальности к договорам, по которым структурное подразделение является исполнителем, уведомление руководства Общества о заключении, и ознакомление с ними работников подразделения;
* организацию конфиденциального делопроизводства в подразделении;
* информирование руководства Общества об инцидентах ИБ, связанных с нарушением работниками структурного подразделения Общества требований по обеспечению ИБ.

### Работники, ответственные за информационную безопасность в структурных подразделениях Общества

По решению руководителя структурного подразделения Общества в подразделении может быть назначен работник, ответственный за обеспечение ИБ в подразделении, перечень обязанностей которого разрабатывается на основании перечня обязанностей, указанного в п.4.1.4, и иных нормативных актов по ИБ Общества.

### Работники Общества

Каждый работник Общества должен быть вовлечен в процессы обеспечения ИБ.

Работники Общества несут персональную ответственность за соблюдение установленных норм и правил по обеспечению ИБ и режима коммерческой тайны.

Работники обязаны:

* соблюдать требования по ИБ при обработке информации, составляющую коммерческую тайну, и иной конфиденциальной информации, а также иной служебной информации;
* использовать информацию, составляющую коммерческую тайну, и иную конфиденциальную информацию Общества, их контрагентов, а также иную защищаемую информацию только в интересах выполнения должностных обязанностей;
* соблюдать иные установленные локальными нормативными актами Общества требования по обеспечению ИБ и режима коммерческой тайны.

Работники, нарушившие установленные требования по ИБ, разгласившие информацию, составляющую коммерческую тайну, и иную конфиденциальную информацию Общества, и их контрагентов, а также работники, по вине которых произошла утрата или искажение защищаемой информации, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Работник, допущенный к информационному активу (системе обработки информации), является пользователем актива (системы).

Конкретные обязанности работников по обеспечению ИБ зависят от занимаемой должности и выполняемых функций и определяются их должностными инструкциями, нормативными и организационно-распорядительными документами Общества, а также инструкциями процессов обеспечения ИБ, в которых они принимают участие.

# Документы по защите информации

Документы по защите информации включают в себя организационно-распорядительные, нормативные, методические, плановые и отчетные документы, регламентирующие организацию, проведение и документирование работ по обеспечению процессов ИБ.

Организационно-распорядительные документы в области обеспечения ИБ издаются (принимаются) в виде решений, приказов, директив и распоряжений.

Нормативные документы устанавливают требования по ИБ и включают в себя политики, положения и регламенты.

Методические документы содержат методы, приемы и способы реализации мероприятий, направленных на выполнение требований по ИБ (инструкции, руководства и т.д.).

Плановые документы включают в себя программы и планы обеспечения ИБ.

В отчетные документы вносятся сведения о результатах работ по обеспечению ИБ, расследованию инцидентов ИБ, контролю выполнения требований по ИБ и эффективности применяемых мер защиты информации, мониторингу состояния ИБ, контролю состояния ИБ. Также должны документироваться правила разграничения доступа к объектам защиты, настройки средств и систем защиты информации, результаты выполнения регламентов работ, связанных с обеспечением ИБ, факты уничтожения информации и прочие сведения, позволяющие подтвердить выполнение установленных требований по ИБ.

В случае, если в системе обработки информации реализация мер защиты, установленных Политикой и другими нормативными документами, невозможна или может привести к нарушению установленных режимов ее функционирования, должны быть приняты иные защитные меры. Замена защитных мероприятий должна быть документирована и согласована для объектов информационной инфраструктуры Общества с руководством и службой по информационной защите.

# Процессы обеспечения ИБ

Политика определяет цели и задачи процессов обеспечения ИБ, а также основные требования к ним.

Для каждого процесса обеспечения ИБ в соответствующих документах системы ИБ, должны быть определены:

* цель процесса обеспечения ИБ, позволяющая обеспечить достижение основных целей ИБ Общества;
* подразделение, ответственное за его организацию и функционирование;
* участвующие в нем подразделения;
* распределение ролей и ответственностей его участников;
* требования по ИБ, описание организационных и технических мероприятий обеспечивающие достижение целей процесса;
* параметры и способы контроля его эффективности.

## Обеспечение ИБ на этапах жизненного цикла объектов информационной инфраструктуры

Жизненный цикл объектов информационной инфраструктуры включает в себя следующие этапы:

* обоснование требований к системе;
* разработка (модернизация) системы;
* ввод системы в эксплуатацию;
* эксплуатация системы;
* вывод системы из эксплуатации.

Требования по ИБ включаются в договоры и контракты на проведение работ или оказание услуг, заключаемые на всех стадиях жизненного цикла систем обработки информации, а также в соответствующую проектную документацию.

С учетом комплексного характера потенциальных угроз информационной инфраструктуре, включающих, в том числе угрозы воздействия вредоносного ПО, преднамеренной и непреднамеренной модификации технологической информации, угрозы форс-мажорного характера, требования по ИБ в обязательном порядке задаются для всех разрабатываемых проектов в сфере информатизации, в том числе для систем обработки информации, не предназначенных для обработки конфиденциальной информации.

Состав предъявляемых к системам обработки информации требований по ИБ и мероприятий по их реализации определяются по результатам классификации систем, с учетом требований законодательства Российской Федерации и актуальных угроз ИБ.

Решение о предъявлении к создаваемой (модернизируемой) системе обработки информации требований по ИБ утверждается ее владельцем (функциональным заказчиком).

Ответственность за включение в техническое задание на создание (модернизацию) систем обработки информации обоснованных требований по ИБ и контроль их выполнения в процессе экспертизы проектной и эксплуатационной документации, испытаний и приемки систем несет владелец объекта защиты.

Технические задания на создание систем обработки информации Общества в части требований по ИБ, согласовываются со службой по информационной безопасности.

Разработка и создание систем обработки информации, в которых обрабатывается информация, составляющая коммерческую тайну, и иная конфиденциальная информация, осуществляется с учетом требований документов, регламентирующих создание автоматизированных систем в защищенном исполнении.

В процессе создания систем обработки информации обеспечивается:

- обоснованная формулировка требований к обеспечению ИБ создаваемых систем в соответствии с действующей нормативной базой;

- разработка проектных решений и мер по защиты информации;

- разработка эксплуатационной документации и организационно-распорядительных документов, регламентирующих порядок работы с защищаемой информацией, в том числе порядок доступа к ней;

- приемка в эксплуатацию, при необходимости с проведением аттестации на соответствие требованиям по ИБ;

- предотвращение внесения недокументированных возможностей в ПО и оборудование.

К разработке, внедрению, аттестации и эксплуатации защищаемых систем обработки информации, применяемых в них средств и систем защиты информации, в установленном порядке привлекаются организации, имеющие право на осуществление соответствующей деятельности с соблюдением требований законодательства Российской Федерации.

При эксплуатации систем обработки информации в первую очередь обеспечивается их защита от следующих факторов:

- несанкционированного доступа к информации, ее модификации или уничтожения;

- неумышленной модификации или уничтожения информации;

- сетевых атак, результатом которых являются отказ в обслуживании или ухудшение обслуживания;

- отказа от авторства, выполненных в системе действий.

Недопустимо внесение изменений в системы обработки информации, приводящих к нарушению их функциональности или появлению недокументированных возможностей.

На стадии вывода из эксплуатации систем обработки информации обеспечивается удаление из содержащихся в них запоминающих устройств конфиденциальной информации, информации используемой средствами обеспечения ИБ, а также информации, несанкционированное использование которой может нанести ущерб деятельности Общества. В случае необходимости, перед удалением такая информация может быть перенесена (скопирована) для дальнейшего использования. Выполнение или организация соответствующих работ осуществляется владельцем системы. Факт удаления информации документируется установленным порядком.

Обеспечение ИБ информационной инфраструктуры Общества осуществляется на всех стадиях жизненного цикла ее объектов с учетом ролей всех вовлеченных в этот процесс сторон (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих организаций и надзорных органов).

## Обеспечение ИБ при эксплуатации систем обработки информации и использовании информационных активов

### Физическая защита объектов информационной инфраструктуры Общества

Физическая защита объектов информационной инфраструктуры Общества и мест их размещения (зданий, помещений, аппаратных шкафов, корпусов средств вычислительной техники и связи) осуществляется в целях предотвращения ущерба, который может быть нанесен в результате несанкционированного физического доступа к объектам информационной инфраструктуры, в том числе к каналам связи, посторонних лиц, а также хищения средств обработки защищаемой информации.

Основными мерами по обеспечению физической защиты являются:

* оборудование помещений, в которых располагаются технические средства систем обработки информации, средствами физической защиты и охраны, исключающими возможность бесконтрольного проникновения в указанные помещения посторонних лиц;
* использование инженерно-технических средств охраны;
* регламентирование и учет доступа в помещения, в которых размещены объекты информационной инфраструктуры (серверные, кроссовые и т.д.), контроль выполнения в указанных помещениях работ, не связанных непосредственно с их обслуживанием и работ, выполняемых сторонними организациями;
* регламентирование и учет вноса/выноса технических средств обработки информации на/с территорию(и) Общества;
* регламентирование и учет размещения объектов информационной инфраструктуры вне контролируемых зон;
* назначение ответственных за физическую сохранность объектов информационной инфраструктуры.

Помещения, в которых располагаются технические средства систем обработки информации, оборудуются средствами пожарной безопасности, вентиляции и кондиционирования.

Технические средства систем обработки информации, размещаемые вне специализированных помещений (серверных, кроссовых и т.п.), должны размещаться в запираемых шкафах или ящиках, физическая целостность которых должна регулярно проверяться.

### Защита территорий, зданий и помещений Общества

В целях обеспечения защиты информации и технических средств обработки, хранения и передачи информации обеспечивается защита территорий, зданий и помещений Общества (включая арендуемые).

В Обществе устанавливается пропускной режим, препятствующий бесконтрольному посещению его охраняемых территорий и зданий.

Здания и помещения Общества обеспечиваются инженерно-техническими средствами охраны и средствами пожарной безопасности.

При проведении работ на охраняемых территориях Общества, в его зданиях и помещениях третьими лицами (сторонними организациями) обеспечивается контроль их деятельности работниками структурных подразделений Общества, сопровождающих указанные работы.

### Организация безопасной эксплуатации средств обработки, хранения и передачи информации

В целях обеспечения ИБ объектов информационной инфраструктуры в Обществе устанавливаются правила безопасной эксплуатации средств обработки, хранения и передачи информации.

Принимаются меры по использованию средств обработки, хранения и передачи информации только по целевому назначению, контролю за изменениями состава и конфигурации ПО и оборудования.

Функции по обеспечению безопасной эксплуатации средств обработки, хранения и передачи информации, включая администрирование встроенных средств безопасности, осуществляются соответствующими администраторами СЗИ.

Правила эксплуатации средств обработки, хранения и передачи информации, используемых в Обществе, определяются локальными нормативными документами Общества.

### Защита от вредоносного программного обеспечения

Защита от вредоносного ПО (антивирусная защита) осуществляется в целях предотвращения проникновения вредоносного программного кода в информационную инфраструктуру Общества, а также его своевременного обнаружения и нейтрализации.

Защита от вредоносного ПО подразумевает построение централизованной многоуровневой (эшелонированной) системы антивирусной защиты, включающей в себя антивирусное ПО, технические и организационные меры защиты.

Система антивирусной защиты должна предусматривать:

* централизованное управление средствами антивирусной защиты;
* установку антивирусного ПО на все объекты информационной инфраструктуры в зависимости от применяемых информационных технологий;
* регулярную установку обновлений антивирусного ПО и баз его вирусных сигнатур;
* протоколирование и аудит событий средств антивирусной защиты;
* регулярный контроль корректности функционирования средств антивирусной защиты.

Рекомендуется использование на разных уровнях системы защиты от вредоносного ПО средств антивирусной защиты различных производителей.

Настройки антивирусного ПО должны предусматривать:

* проверку в режиме реального времени загружаемых в оперативную память АРМ и серверов данных и исполняемого кода;
* проверку подключаемых к АРМ и серверам съемных носителей информации;
* регулярное проведение полных антивирусных проверок накопителей информации АРМ и серверов;
* регистрацию событий безопасности при обнаружении или подозрении на обнаружение вирусного заражения;
* автоматическое уведомление соответствующих должностных лиц, ответственных за обеспечение антивирусной защиты при обнаружении или подозрении на обнаружение вирусного заражения;
* запрет пользователям производить остановку работы средств антивирусной защиты или их настройку.

В качестве дополнительных мер антивирусной защиты, а также в случаях, когда по техническим причинам применение антивирусного ПО для защиты АРМ или серверов невозможно, должны быть приняты иные технические и организационные меры защиты от вредоносного ПО.

В числе указанных мер защиты могут быть использованы следующие:

* полная антивирусная проверка внешним средством антивирусной защиты накопителей АРМ и серверов;
* антивирусная проверка ПО, устанавливаемого на АРМ и серверы;
* организационный и/или технический запрет использования на АРМ и серверах съемных носителей информации без их предварительной проверки средствами антивирусной защиты;
* организация повседневной работы администраторов АРМ и серверов под учетными записями, права доступа которых не позволяют устанавливать ПО или изменять настройки операционной системы;
* отключение служб, неиспользуемых в работе АРМ или серверов;
* блокировка специализированным ПО, либо физическая блокировка или демонтаж портов ввода вывода информации (USB), приводов съемных носителей информации или их отключение соответствующими настройками BIOS/UEF1 или ОС АРМ и серверов;
* ограничение сетевого взаимодействия защищаемых АРМ и серверов с другими вычислительными сетями, АРМ или серверами.

О фактах обнаружения вирусной активности (в том числе активного вредоносного ПО) или следов их деструктивного воздействия информируется служба по информационной защите, принимаются меры по его нейтрализации, устраняются последствия действии вредоносного ПО, проводится расследование причин вирусного заражения.

При необходимости допускается на период нейтрализации атаки вредоносного ПО приостанавливать функционирование зараженных систем обработки информации или производить их отключение от вычислительной сети Общества.

### Резервирование информационных активов и технических средств обработки, хранения и передачи информации

**6.2.5.1. Резервное копирование информационных активов**

В целях обеспечения возможности восстановления информационных активов в случае их утраты или нарушения целостности в Обществе осуществляется их резервирование.

Способ и периодичность резервного копирования, а также сроки хранения резервных копий определяются проектной и эксплуатационной документацией на системы обработки информации.

**6.2.5.2. Резервирование средств обработки, хранения и передачи информации**

В целях обеспечения бесперебойного функционирования информационной инфраструктуры Общества рекомендуется резервирование критически важных средств обработки, хранения и передачи информации, а также определение порядка восстановления работоспособности элементов информационной инфраструктуры с использованием резервных аппаратных и программных средств.

Технические решения по резервированию критически важных средств обработки, хранения и передачи информации должны быть документированы в установленном порядке.

### Обеспечение сетевой безопасности

В целях обеспечения защиты информации и устойчивого функционирования информационной инфраструктуры в Обществе осуществляются мероприятия по обеспечению сетевой безопасности.

Обеспечение сетевой безопасности достигается защитой локальной вычислительной сети Общества от неправомочных действий пользователей и посторонних лиц.

Обеспечение сетевой безопасности реализуется, в том числе следующими мерами:

* использованием межсетевых экранов на границах между ЛВС Общества и внешними сетями;
* физическим или логическим (с использованием маршрутизаторов, межсетевых экранов, технологий виртуальных ЛВС) сегментированием ЛВС Общества;
* фильтрацией сетевого трафика между различными сегментами вычислительных сетей;
* управлением доступом к сетевому оборудованию;
* защитой сетевых потоков управления сетевом оборудованием;
* использованием систем обнаружения и предотвращения вторжений;
* мониторингом подключаемых к вычислительным сетям сетевых устройств и запретом несанкционированного подключения таких устройств, отключением неиспользуемых сетевых портов на сетевом оборудовании;
* физической защитой элементов сетевой инфраструктуры;
* резервированием элементов сетевой инфраструктуры;
* применением средств криптографической защиты информации при передаче конфиденциальной информации за пределы контролируемых зон;
* обеспечением безопасности при использовании технологий удаленного сетевого доступа и беспроводных сетей;
* организацией мониторинга состояния работоспособности сетевого оборудования.

В рамках обеспечения сетевой безопасности принимаются меры по регламентированию и документированию межсетевого информационного обмена между объектами информационной инфраструктуры.

Указанные меры реализуются структурными подразделениями Общества по направлениям деятельности в соответствии с локальными нормативными документами Общества области ИБ и требованиями эксплуатационной документации.

Правила межсетевого экранирования должны запрещать все сетевые взаимодействия, за исключением тех, которые необходимы для реализации бизнес-процессов или функционирования вычислительной инфраструктуры.

В составе сетевой инфраструктуры должны быть выделены следующие сегменты:

* демилитаризованные зоны;
* сегменты управления объектами информационной инфраструктуры;
* серверные сегменты;
* пользовательские сегменты;
* сегменты для информационных систем и сервисов с высоким уровнем критичности;
* сегменты разработки и тестирования информационных систем и сервисов.

Доступные из внешних сетей серверы Общества, в том числе почтовые серверы, веб-серверы, серверы удаленного доступа и другие, должны размещаться в демилитаризованных зонах, отделенных межсетевыми экранами как от внутренних сегментов сетей Общества, так и от внешних сетей.

При осуществлении управления сетевым оборудованием и средствами защиты без использования выделенной сети управления осуществляется криптографическая защита каналов управления.

Доступ к управлению сетевым оборудованием предоставляется только его администраторам и администраторам ИБ.

Обеспечение безопасности при использовании технологий удаленного сетевого доступа реализуется выполнением следующих мероприятий:

* принятием решения об использовании удаленного доступа на основе анализа связанных с ним рисков ИБ и исходя из необходимости осуществления такого доступа к информационным активам;
* определением перечня информационных активов, к которым предоставляется удаленный доступ и лиц, которым такой доступ разрешен, согласованием указанных перечней с руководством ИТ и службой по информационной безопасности;
* прохождением пользователями процедур аутентификации на шлюзе удаленного доступа, размещаемом в демилитаризованной зоне;
* использованием при удаленном подключении средств усиленной аутентификации и технологии, обеспечивающей криптографическую защиту передаваемой информации.

Безопасность использования беспроводных сетей обеспечивается реализацией следующих мер:

* принятием решения об использовании беспроводных сетей на основе анализа связанных с ними рисков ИБ;
* регламентацией подключения пользовательских устройств к беспроводной сети;
* физической защитой точек беспроводного доступа;
* минимизацией уровня передаваемого сигнала для исключения его распространения за пределы контролируемой зоны;
* разделением вычислительных сетей и подключаемых к ним беспроводных сетей с помощью межсетевых экранов;
* подключением к беспроводным сетям абонентских устройств после прохождения процедуры аутентификации;
* обнаружением сетевых атак, в том числе контролем попыток подключения к беспроводной сети.

### Обеспечение ИБ при взаимодействии с сетью Интернет

Обеспечение ИБ при взаимодействии с сетью Интернет осуществляется с целью предотвращения случайной или преднамеренной утечки защищаемой информации из ЛВС Общества, а также предотвращения сетевых атак на ЛВС Общества со стороны злоумышленников.

При обеспечении безопасного взаимодействия информационной инфраструктуры Общества с сетью Интернет применяются следующие первоочередные меры защиты:

- предоставление работникам доступа к сети Интернет только при наличии производственной необходимости;

- предоставление доступа пользователям к сети Интернет только после прохождения ими аутентификации;

- организация взаимодействия ЛВС Общества с сетью Интернет через единый шлюз, с принятием мер по обеспечению сетевой безопасности;

- выбор доверенного поставщика услуг доступа в сеть Интернет;

- скрытие при взаимодействии с сетью Интернет внутренней адресации и структуры информационной инфраструктуры Общества;

- выделение ресурсов ЛВС, к которым осуществляется доступ из сети Интернет, в изолированную с помощью межсетевого экрана подсеть (демилитаризованную зону);

- запрет несанкционированного использования ПО, реализующего скрытые каналы передачи данных или сетевую трансляцию IP-адресов и портов.

Обеспечение безопасного использования сети Интернет с АРМ и серверов осуществляется за счет:

- настройки межсетевых экранов, прокси-серверов, исключающей несанкционированную передачу информации между сетью Интернет и защищаемыми АРМ или серверами;

- учета АРМ и серверов, на которых ведется обработка конфиденциальной информации;

- контролем сетевого трафика в сеть Интернет на предмет выявления передачи в незащищенном виде конфиденциальной информации (в том числе с использованием DLP-систем);

- шифрованием сообщений электронной почты. содержащих конфиденциальную информацию;

- проверки сетевого трафика на отсутствие вредоносного ПО и спама.

### Обеспечение ИБ при использовании съемных носителей информации, мобильных и коммуникационных устройств

При использовании съемных носителей информации, мобильных и коммуникационных устройств принимаются защитные меры в целях предотвращения несанкционированного доступа к информационным активам, а также проникновения вредоносного ПО) в информационную инфраструктуру Общества, установления несанкционированных каналов взаимодействия с сетью Интернет, кражи или разглашения информации ограниченного доступа и защищаемой информации.

Обеспечение ИБ при использовании съемных носителей информации, мобильных и коммуникационных устройств реализуется принятием следующих мер:

- исключением подключения незарегистрированных в установленном порядке съемных носителей информации к АРМ, серверам и вычислительным сетям;

- исключением использования не проверенных средствами антивирусной защиты съемных носителей информации и мобильных устройств на АРМ, серверах и в вычислительных сетях;

- маркировкой и учетом съемных носителей конфиденциальной информации в соответствии с установленным в Обществе порядком;

- утилизацией съемных носителей информации, мобильных устройств, при выводе их из эксплуатации, с обеспечением гарантированного уничтожения содержащейся на них конфиденциальной информации;

- регистрацией и учетом служебных съемных носителей информации, мобильных и коммуникационных устройств, принятием мер по защите их от вредоносного ПО и кражи;

- организацией регулярного контроля сохранности (наличия) служебных съемных носителей информации, мобильных и коммуникационных устройств.

Рекомендуется осуществлять шифрование защищаемой информации, содержащейся на съемных носителях информации и мобильных устройствах, а также принятие мер по централизованному контролю информации, записываемой на данные устройства.

Для управления подключением к АРМ и серверам съемных носителей информации, мобильных и коммуникационных устройств целесообразно применение специализированных программных решений, позволяющих исключить несанкционированное использование на указанных АРМ и серверах устройств и портов ввода-вывода информации.

Применение в информационной инфраструктуре Общества съемных носителей информации, мобильных и коммуникационных устройств, в том числе принадлежащих по праву собственности работникам Общества, без принятия установленных мер защиты запрещено.

### Защита ПО

В целях поддержания работоспособности ПО, предотвращения сетевых и вирусных атак, соблюдения законодательства в области авторских и смежных нрав в Обществе организуется защита ПО.

В целях поддержания работоспособности ПО в Обществе осуществляются меры защиты ПО, включающие:

* регламентирование порядка и контроль использования ПО;
* резервирование конфигураций ПО;
* устранение уязвимостей путем обновления состава и конфигурации ПО в соответствии с рекомендациями разработчика.

Новое ПО и все обновления его состава и конфигурации принимаются в эксплуатацию только после успешного прохождения тестирования на совместимость с существующей информационной инфраструктурой, а также проверки функционирования на тестовой среде, в качестве которой служит специально подготовленная среда. Обновление состава и конфигурации ПО возлагается на работников структурных подразделений Общества, отвечающих за его эксплуатационное сопровождение.

Защите подлежит прикладное ПО, системное ПО серверов, АРМ и сетевого оборудования, а также ПО, обеспечивающее низкоуровневые функции аппаратных средств систем обработки информации («прошивки» контроллеров и дисковых хранилищ, BIOS/UEFI материнских плат и т.д.).

При использовании ПО должны соблюдаться условия лицензионных договоров (соглашений), что обеспечивается регулярной инвентаризацией использующегося в информационной инфраструктуре ПО и мониторингом соответствия условий его использования лицензионным соглашениям.

На АРМ и серверах Общества запрещается:

* установка (использование) ПО (сервисов), не требующегося для работы АРМ и серверов или не являющегося необходимым для функционирования бизнес-процессов Общества;
* необоснованный запуск ПО (служб и сервисов), от имени учетных записей, обладающих расширенными привилегиями, которые не требуются для работы указанного ПО;
* установка, хранение или использование вредоносных программ и ПО обхода технических средств защиты.

### Регистрация и учет событий ИБ

В целях своевременного выявления нарушений ИБ, контроля действий администраторов и пользователей систем обработки информации, обеспечения возможности проведения расследования инцидентов ИБ в Обществе осуществляется регистрация и учет событий ИБ.

Регистрация и учет событий ИБ осуществляется в журналах средств защиты информации, технических средств обработки, хранения и передачи информации.

Журналы событий регулярно анализируются администраторами, администраторами СЗИ и администраторами ИБ объектов информационной инфраструктуры. Журналы событий могут подвергаться автоматизированному анализу в целях оперативного выявления возможных инцидентов ИБ.

Перечень событий ИБ, подлежащих регистрации, период времени хранения журналов событий ИБ, периодичность контроля указанных журналов, порядок реагирования на выявляемые события ИБ и другие аспекты контроля событий ИБ устанавливаются локальными нормативными актами Общества или технической документации объектов информационной инфраструктуры.

### Криптографическая защита информации

В целях обеспечения конфиденциальности, целостности и аутентичности обрабатываемой, хранимой и передаваемой информации в информационной инфраструктуре Общества применяются сертифицированные установленным порядком средства криптографической защиты информации.

Электронные документы, для которых необходимо обеспечить целостность и аутентичность, защищаются с помощью средств электронной подписи.

При передаче конфиденциальной информация по каналам связи за пределы контролируемых зон, должны применяться средства криптографической защиты информации.

Криптографическая защита информации в приложениях, поддерживающих технологию открытых ключей, может реализовываться с помощью сервисов электронной подписи и криптографической защиты.

При использовании съемных носителей информации и мобильных устройств информация ограниченного доступа, хранимая на них, подлежит обязательной защите с использованием криптографической защиты.

## Контроль доступа

### Управление доступом пользователей

В целях обеспечения безопасности и устойчивого функционирования информационной инфраструктуры в Обществе осуществляется управление доступом пользователей к информационным ресурсам, прикладным системам и техническим средствам в ее составе.

Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных обязанностей. Наделение пользователей правами доступа и привилегиями основывается на установленной в Обществе формализованной процедуре предоставления прав доступа. Принцип разделения полномочий при наделении пользователей правами обеспечивается ведением матриц доступа к информационным ресурсам и автоматизированным системам обработки, хранения и передачи информации. Права доступа и привилегии пользователей подлежат регулярному пересмотру.

Допускается неформализованное наделение полномочиями авторизованных пользователей при организации доступа к справочной информации, не содержащей сведения, составляющие коммерческую тайну, и иную конфиденциальную информацию, а также к общедоступной информации.

Все реквизиты доступа к элементам информационной инфраструктуры Общества имеют однозначную персонификацию.

Порядок управления доступом пользователей к информационным ресурсам определяется владельцем объекта информационной инфраструктуры или информационного актива и документируется в установленном порядке.

### Ответственность пользователей при доступе к информационным ресурсам

В целях предотвращения несанкционированного доступа, а также компрометации или утраты информации и средств обработки информации, определяется ответственность пользователей по соблюдению правил доступа при использовании АРМ.

Пользователи несут ответственность за соблюдение конфиденциальности и сохранности средств и параметров аутентификации.

Пользователям запрещено работать под чужими учетными записями, а также сообщать свои пароли или передавать аппаратные средства аутентификации другим лицам. При временном оставлении АРМ пользователем принимаются меры по блокированию сеанса работы для защиты от несанкционированного доступа.

Парольная политика, правила использования паролей и средств усиленной аутентификации определяются локальными нормативными и организационно-распорядительными документами Общества в области ИБ. Ответственность пользователей за выполнение установленных правил ИБ включается в текст трудовых договоров и функциональных обязанностей работников Общества.

## Контроль защищенности

В целях своевременного и эффективного реагирования на опубликованные и выявленные уязвимости, а также устранения недостатков в конфигурации технических средств обработки, хранения и передачи информации в информационной инфраструктуре Общества осуществляется контроль защищенности ОЗ.

Организация контроля защищенности должна включать в себя составление перечня объектов контроля защищенности, с указанием их проверяемых параметров, регламентирование порядка контроля защищенности и периодичности его проведения.

Проверка защищенности должна включать в себя:

* получение из внешних источников информации (производителей ОЗ, специализированных сайтов сети Интернет и др.) сведений об уязвимостях программного обеспечения, анализ указанных сведений и их использование в ходе проверки защищенности;
* выявление уязвимостей объектов информационной инфраструктуры, в том числе с использованием автоматизированных средств;
* анализ конфигурационных файлов и настроек систем обработки информации.

При проведении инструментального контроля защищенности должны приниматься меры, исключающие его негативное воздействие на информационную инфраструктуру.

По результатам анализа защищенности должны приниматься меры, нейтрализующие выявленные уязвимости и недостатки.

Порядок проведения контроля защищенности устанавливается в локальных нормативных актах Общества.

## Обеспечение соответствия требованиям по ИБ

В целях минимизации возможного ущерба от претензий со стороны органов государственной власти в Обществе принимаются меры по обеспечению соответствия требованиям законодательства Российской Федерации и федеральных органов исполнительной власти в области защиты информации и обеспечения ИБ.

В Обществе осуществляются меры по защите информации, доступ к которой ограничен федеральными законами (информации ограниченного доступа), включая информацию, составляющую коммерческую тайну, и персональные данные.

В Обществе не допускается обработка информации, создание, хранение или распространение которой запрещено законодательством Российской Федерации.

В Обществе допускается эксплуатация только ПО, полученного на законных основаниях, а также принимаются меры по соблюдению авторских прав и условий лицензионных соглашений.

При осуществлении Обществом деятельности на территории иностранных государств, должны выполнятся требования национального законодательства в области ИБ указанных государств.

### Обеспечение режима коммерческой тайны

В Обществе установлен режим коммерческой тайны, предусматривающий правовые, организационные и технические меры по защите информации, составляющей коммерческую тайну, и иной конфиденциальной информации.

Меры по защите информации, составляющей коммерческую тайну, и иной конфиденциальной информации регламентируются локальными нормативными и организационно-распорядительными документами Общества в области ИБ.

### Обеспечение защиты персональных данных

В Обществе установлен порядок обработки персональных данных в соответствии с требованиями законодательства Российской Федерации, а также принимаются правовые, организационные и технические меры по обеспечению их безопасности.

Порядок обработки персональных данных и перечень мер по их защите регламентируется нормативными и организационно-распорядительными документами Общества.

Выбор мер по обеспечению безопасности персональных данных при их обработке в информационных системах должен осуществляться на основе законодательства Российской Федерации в области персональных данных, нормативных и руководящих документов федеральных органов исполнительной власти Российской Федерации.

Распределение обязанностей и полномочий при обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных определяется Положением о реализации мер по обеспечению защиты персональных данных работников в ООО «My Company», утвержденное приказом Общества от 01.09.2022 № 1/01-09/2022.

### Организация работы с персоналом по вопросам ИБ

**6.5.3.1. Обеспечение ИБ при заключении и во время действия трудового договора**

Организация работы с персоналом по вопросам ИБ осуществляется с целью обеспечения ИБ при приеме на работу новых работников, выполнении ими своих должностных обязанностей и увольнении.

В целях повышения уровня ИБ все работники Общества при приеме на работу проходят в отделе кадров первичный инструктаж, на котором до них доводятся требования по ИБ и информация об ответственности за нарушение указанных требований.

Обязанности работников Общества по обеспечению ИБ и соблюдению требований ИБ устанавливаются их должностными инструкциями и трудовым договором, а также конкретизируются нормативными и организационно-распорядительными документами Общества в области ИБ.

С каждым работником при его трудоустройстве в Общество заключается договор о конфиденциальности.

В Обществе обеспечивается сохранность заключенных договоров о конфиденциальности.

Работники Общества, непосредственно осуществляющие обеспечение ИБ:

* регулярно проходят повышение квалификации,
* знакомятся с изменениями в федеральном законодательстве Российской Федерации, нормативных и организационно-распорядительных документах Общества в области ИБ;
* информируют работников структурных подразделений Общества об изменениях в содержании организационного и технического обеспечения ИБ в Обществе.

Поддержание и повышение квалификации работников, обеспечивающих ИБ, реализуется существующей в Обществе системой переподготовки и повышения квалификации кадров.

Мероприятия по повышению осведомленности работников в области ИБ включают:

- разработку и доведение до работников информационных материалов со сведениями об актуальных угрозах ИБ и основными требованиями по ИБ;

- размещение документов, содержащих требования по ИБ, в доступном для пользователей месте на внутреннем веб-портале Общества.

**6.5.3.2. Обеспечение безопасности при увольнении и при изменении условий трудового договора**

В целях обеспечения ИБ при увольнении работника Общества и при изменении его условий трудового договора в Обществе осуществляется контроль возврата информационных носителей, средств обработки, хранения и передачи информации, своевременного изменения и прекращения прав доступа работников к объектам информационной инфраструктуры Общества.

Порядок реализации указанных мер определяется нормативными документами Общества в области ИБ, а также эксплуатационными регламентами соответствующих объектов информационной инфраструктуры Общества.

Инструктаж увольняемых работников о принятых ими обязательствах по соблюдению в тайне конфиденциальных сведений и доведение до них срока сохранения в тайне сведений, с которыми они были ознакомлены, выполняется отделом кадров. При увольнении работника (изменении условий трудового договора) его права доступа к информационным активам незамедлительно аннулируются (приводятся в соответствие с новыми условиями).

Отдел кадров своевременно уведомляет ИТ и ИБ об увольнении (изменении условий трудового договора) работников.

Работники Общества, имеющие доступ к информации, подлежащей защите, за разглашение и утрату такой информации, а также за нарушение установленного порядка обеспечения ИБ несут ответственность в соответствии с действующим законодательством Российской Федерации.

### Обеспечение ИБ при работе с контрагентами

Обеспечение ИБ при работе со сторонними организациями или физическими лицами (далее - контрагенты) осуществляется с целью защиты информационных активов и информационной инфраструктуры Общества от деструктивных и противоправных действий недобросовестных или злонамеренных работников контрагентов, а также с целью правовой защиты конфиденциальной информации Общества.

При организации доступа контрагентов к защищаемым информационным активам в Обществе осуществляются следующие мероприятия по обеспечению ИБ:

* регламентация предоставления доступа контрагентам к конфиденциальной информации или информационной инфраструктуре;
* заключение соглашении (договоров) о конфиденциальности с контрагентами, которым предоставляется доступ к конфиденциальной информации или информационной инфраструктуре Общества.

При оказании контрагентом Обществу услуг, предусматривающих доступ к конфиденциальной информации или информационной инфраструктуре Общества, договор на оказание соответствующих услуг должен предусматривать:

* обязанность контрагента по обеспечению конфиденциальности информации, ставшей ему известной при оказании услуг, в соответствии с заключенным между ним и Обществом соглашением (договором) о конфиденциальности к договору на оказание услуг;
* обязательства контрагента по соблюдению им в ходе выполняемых работ установленных в Обществе требований по ИБ;
* обязательства контрагента по выполнению требований Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» в случае, если персональные данные, оператором которых является Общество, доступны ему в ходе оказания услуг.

Если оказываемые контрагентом услуги являются аутсорсингом и связаны с созданием, модернизацией, обслуживанием информационной инфраструктуры или систем обработки информации Общества в договор на оказание соответствующих услуг дополнительно включаются следующие положения:

предоставление услуг по обслуживанию (поддержке, администрированию и т.п.) информационной инфраструктуры или систем обработки информации на основании соглашения об уровне обслуживания (service-level agreement - SLA). Содержание SLA рекомендуется определять исходя из положений ГОСТ Р ИСО/МЭК 20000-2-2010;

* учет в SLA необходимости выполнения контрагентом требований по ИБ в ходе оказания услуг;
* создание и соблюдение регламентов и инструкций, позволяющих контрагенту реализовать, а Обществу контролировать исполнение SLA;
* - соблюдение контрагентом требований законодательства Российской Федерации в области лицензирования - наличие у контрагента лицензий ФСТЭК России и ФСБ России на осуществляемые им по договору виды деятельности;
* право Общества на осуществление мониторинга обслуживаемой контрагентом информационной инфраструктуры (системы обработки информации), участие Общества в подготовке заключений по кандидатам на замещение вакантных должностей у контрагента, занимая которые его работники привлекаются для исполнения работ по оказанию услуг Общества. Также рекомендуется предусматривать право Общества на проведение аудита СОИБ контрагента.

Порядок представления информации органам государственной власти регламентируются нормативными и организационно-распорядительными документами Общества в области ИБ.

## Предотвращение утечки защищаемой информации по техническим каналам

Основными задачами при обеспечении защиты информации от утечки по техническим каналам являются выявление и пресечение возможных каналов утечки.

Применяются следующие организационно-технические меры противодействия утечке защищаемой информации по техническим каналам:

* определение перечня защищаемых помещений;
* регламентирование порядка проведения деловых встреч и переговоров, ведения телефонных разговоров;
* регламентирование порядка проведения обследований защищаемых помещений и технических средств на предмет установления каналов утечки;
* обеспечение режима доступа в служебные помещения;
* исключение возможности установки посторонних (внештатных) предметов на внешней стороне ограждающих конструкций защищаемых помещений и выходящих из них коммуникаций (систем отопления, вентиляции, кондиционирования);
* оборудование защищаемых помещений специальными средствами защиты от утечки информации;
* использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;
* размещение объектов защиты на максимально возможном расстоянии от границы контролируемой зоны;
* использование защищенных каналов связи;
* оборудование служебных помещений средствами разграничения доступа.

# Ответственность руководства и работников Общества

Руководство Общества отвечает за состояние ИБ в Обществе и обеспечивает реализацию настоящей Политики, включая регулярный контроль ее исполнения, актуализации и выделения, необходимых для обеспечения ИБ ресурсов, а также организацию осведомленности и обучения работников Общества в области обеспечения ИБ.

На руководителей структурных подразделений Общества возлагается ответственность за:

* соблюдение работниками структурного подразделения режима коммерческой тайны;
* соответствие полномочий работников подчиненного структурного подразделения по доступу к конфиденциальной информации, информационным активам Общества, сетевым сервисам и ресурсам ЛВС Общества их должностным обязанностям.

Ответственность за выполнение норм и правил обеспечения ИБ при эксплуатации конкретного объекта информационной инфраструктуры Общества возлагается на работников, эксплуатирующих такой объект.

Работники Общества обязаны выполнять следующие общие требования по ИБ:

* соблюдать требования настоящей Политики, других локальных нормативных и организационно-распорядительных документов Общества в области ИБ;
* использовать служебные технические средства обработки информации только в служебных целях;
* в установленном порядке информировать руководство Общества и службу ИБ о выявленных инцидентах ИБ.

Работники Общества, не выполняющие требования настоящей Политики или требования локальных нормативных и организационно-распорядительных документов Общества в области ИБ, могут быть привлечены к ответственности в установленном порядке.

# Порядок пересмотра Политики

Настоящая Политика пересматривается с периодичностью не реже чем один раз в три года. При необходимости в нее вносятся изменения.

При пересмотре Политики учитываются результаты контроля эффективности обеспечения ИБ / аудита ИБ за предыдущий период.

Процедура пересмотра Политики включает:

* анализ и выявление несоответствий действующей Политики текущим условиям;
* разработку предложений по совершенствованию Политики;
* утверждение новой редакции Политики.

При осуществлении процедуры пересмотра учитываются:

* указания руководства Общества по совершенствования СОИБ;
* результаты контроля состояния ИБ в Обществе, расследования инцидентов ИБ, контроля соблюдения требований по ИБ и оценки эффективности принимаемых мер защиты информации;
* предложения структурных подразделений Общества по совершенствованию процессов обеспечения ИБ;
* изменения в организационно-штатной структуре Общества и в его информационной инфраструктуре;
* изменения в законодательной и нормативной базе по ИБ, произошедшие с момента утверждения предыдущей редакции Политики;
* результаты анализа произошедших инцидентов ИБ, а также уязвимости и угрозы, выявленные в Обществе за время, прошедшее с момента утверждения предыдущей редакции Политики;
* изменения в управлении ИБ, включая изменения в распределении ресурсов и обязанностей при обеспечении ИБ.