|  |
| --- |
|  |

Оглавление

[1. **Общие положения** 2](#_Toc54029198)

[2. **Список терминов и определений** 3](#_Toc54029199)

[3. **Описание объекта защиты** 5](#_Toc54029200)

[4. **Цели и задачи деятельности по обеспечению информационной безопасности** 5](#_Toc54029201)

[5. **Угрозы информационной безопасности** 6](#_Toc54029202)

[6. **Модель нарушителя информационной безопасности** 7](#_Toc54029203)

[7. **Основные положения по обеспечению информационной безопасности** 7](#_Toc54029204)

[8. **Организационная основа деятельности по обеспечению информационной безопасности** 8](#_Toc54029205)

[9. **Ответственность за соблюдение положений Политики** 9](#_Toc54029206)

[10. **Контроль за соблюдением положений Политики** 10](#_Toc54029207)

[11. **Заключительные положения** 10](#_Toc54029208)

# Общие положения

Настоящая политика информационной безопасности ООО «Арктур» (далее – Общество) определяет официально принятую систему взглядов на проблему обеспечения информационной безопасности в автоматизированных системах. Политика содержит в себе структурированное изложение целей и задач защиты, способы достижения требуемого уровня информационной безопасности, технологических и организационных аспектов обеспечения информационной безопасности в АС.

Политика учитывает современное состояние и перспективы развития АС, цели и задачи, правовые основы её создания и эксплуатации, а также анализа угроз безопасности.

Правовой основой Политики являются:

* Конституция Российской Федерации;
* Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных»;
* Закон Российской Федерации № 5485-1 от 21.07.1993 «О государственной тайне»;
* Федеральный закон № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон № 99-ФЗ от 04.05.2011 «О лицензировании отдельных видов деятельности»;
* Доктрина информационной безопасности Российской Федерации (5 декабря 2016 г. №646);
* Кодекс Российской Федерации об административных правонарушениях (от 30.12.2001 N 195-Ф3);
* Внутренние нормативно – методические и организационно – распорядительные документы;
* Федеральный закон № 126-ФЗ от 07.07.2003 «О связи»;

Основные положения Политики распространяются на все структуры и подразделения Общества. Основные положения Политики могут быть распространены также на подразделения других организаций и учреждений (в том числе дочерние), осуществляющие взаимодействующие с АС в качестве поставщиков и потребителей (пользователей) информации АС.

Политика является основой для:

* Формирования и проведения единой политике в основе информационной безопасности в АС;
* Принятия управленческих решений и разработки практических мер по воплощению политики информационной безопасности и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз информационной безопасности;
* Разработки стратегии информационной безопасности Общества, включая цели, задачи и комплекс мер по её практической реализации;

Требования настоящей Политики распространяются на всех сотрудников Фирмы (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).



# Список терминов и определений

**Автоматизированная система (АС)** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Администратор информационной безопасности** – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

**Доступ к информации** – возможность получения информации и ее использования.

**Информационные ресурсы** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

**Источник угрозы** – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

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

**Угрозы информации** – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

**Конфиденциальность** – доступ к информации только авторизованных пользователей.

**Локальная вычислительная сеть** – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

**Несанкционированный доступ к информации** – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

**Политика информационной безопасности** – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в Учреждении для обеспечения его информационной безопасности.

**Пользователь локальной вычислительной сети** – сотрудник организации (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

**Рабочая станция** – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

**Личный профиль пользователя** – учётная запись в вычислительных системах, принадлежащих компании

**Ответственный за техническое обеспечение** – сотрудник организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети Министерства труда, социального развития и занятости населения Республики Алтай и ПК.

**Уязвимость** – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности Общества при реализации угроз в информационной сфере.

**Программное обеспечение** – совокупность прикладных программ, установленных на сервере или ЭВМ.

**Целостность информации** – состояние защищенности информации, характеризуемое способностью, АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

# Описание объекта защиты

Объекты информационной безопасности – это компоненты информационной среды, угрозы которым представляют опасность для застрахованных, страхователей, работников, акционеров Общества и т.д.

Основными объектами информационной безопасности в Обществе являются:

* информационные ресурсы с ограниченным доступом, составляющие коммерческую, врачебную, служебную тайну, персональные данные, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления;
* процессы обработки информации в АС – информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков, администраторов и пользователей АС;
* Сотрудники Общества, являющиеся разработчиками и пользователями информационных систем Общества;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты АС;

# Цели и задачи деятельности по обеспечению информационной безопасности

Целью деятельности по обеспечению информационной безопасности Общества является снижение угроз информационной безопасности до приемлемого для Общества уровня.

Субъектами правоотношений при использовании АС и обеспечении информационной безопасности являются:

* Должностные лица и работники Общества и его подразделений, как пользователи АС и поставщики информации в неё в соответствии с их должностными обязанностями;
* Юридические и физические лица, информация о которых накапливается, хранится и обрабатывается в АС;
* Другие физические и юридические лица, задействованные в процессе создания и регулировки работы АС;
* ИТ подразделения общества, обеспечивающие эксплуатацию систем обработки информации;

Основные задачи деятельности по обеспечению информационной безопасности Общества:

* Выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
* Регистрация действий пользователя при использовании ресурсов АС и периодический контроль корректности действий пользователя системы;
* Запись всех исходящих и входящих звонков с телефона организации Общества;
* Обеспечение идентификации всех пользователей, участвующих в обмене информации (подтверждение подлинности отправителя и получателя);
* Выявление источников угроз информационной безопасности, способствующих нанесению любого ущерба Общества;

# Угрозы информационной безопасности

Все потенциальные угрозы безопасности информации делятся на три класса, по сути, их возникновения: антропогенные, техногенные и естественные (природные).

Естественные (природные) угрозы – угрозы, вызванные воздействиями на информационную систему и ее компоненты физических процессов техногенного характера и стихийных природных явлений, независящих от человека.

Техногенные угрозы – угрозы, определяемые технократической деятельностью человека и развитием цивилизации. Они напрямую зависят от свойств техники. Их подразделяют на внутренние и внешние.

К внутренним источникам относятся некачественные технические и/или программные средства обработки информации, вспомогательные средства, а также вредоносное программное обеспечение и аппаратные закладки.

К внешним источникам относятся инфраструктурные элемента информационных систем: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (канализация, отопление, водоснабжение и пр.).

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Антропогенные источники угроз по отношению к информационной системе могут быть как внешними, так и внутренними.

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники. Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании информационной системы предприятия и ее элементов, ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в информационной системе. К таким источникам можно отнести персонал поставщиков различного рода услуг, персонал надзорных организаций и аварийных служб и т.п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или халатности, из любопытства, но без злого умысла

Преднамеренные источники проявляются в корыстных устремлениях нарушителей. Основная цель таких источников – умышленная дезорганизация работы, вывод систем предприятия из строя, искажение информации за счет проникновения в информационные ресурсы предприятия путем несанкционированного доступа.

# Модель нарушителя информационной безопасности

Нарушитель – лицо, которое предприняло попытку выполнения запрещенных операций по ошибке, незнанию или осознанно со злым умыслом или без такового и использующее для этого различные возможности, методы и средства.

По отношению к Обществу нарушители могут быть разделены на внешних и внутренних нарушителей.

Внутренние нарушители:

* Работник Общества, зарегистрированный как пользователь системы;
* Работник Общества, не допущенные к работе с АС;
* Персонал, обслуживающий технические средства АС;
* Сотрудники компаний, принадлежащих Обществу;
* Руководители разных уровней;

Внешние нарушители:

* Бывшие сотрудники Общества;
* Клиенты Общества;
* Представители организаций, взаимодействующие с угрожающей по вопросам технического обеспечения;
* Лица, случайно или специально проникшие в корпоративную информационную среду Общества из внешних телекоммуникационных сетей (хакеры);
* Члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;

Ограничения и предположения о характере действий возможных нарушений:

* Подозрительная активность внутреннего нарушителя, перехваченная с его персонального компьютера;
* Несанкционированные действия являются следствием ошибок пользователей, и других лиц Общества;
* Скрытие несанкционированных действий от сотрудников Общества;
* Любой вид договоренности внешнего нарушителя с сотрудником Общества;

# Основные положения по обеспечению информационной безопасности

* 1. Все сотрудники Общества должны четко знать и выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности.
  2. При вступлении в должность нового сотрудника, его начальник должен организовать ознакомление с необходимыми документами, а также провести обучение навыкам выполнения процедур, необходимых для санкционированного использования ресурсов Общества
  3. Сотрудник Общества и его подразделений обязан обеспечивать сохранность идентификаторов (электронных ключей) и не допускать людей, не причастным к Обществу, не передавать персональную информацию третьим лицам
  4. Сотрудник Общества должен самостоятельно обеспечивать сохранность и функциональность рабочего оборудования, оставляемого без присмотра
  5. Сотрудникам запрещается установление постороннего программного обеспечения, подключать мобильные устройства и носители информации, а также записывать на них защищаемую информацию
  6. Сотрудникам запрещается разглашать защищаемую информацию, которая им стала известна в результате трудовой деятельности, при работе с информационными системами Общества, третьим лицам
  7. При работе с персональным софтом Общества (MS Office, 1С) сотрудник обязан обеспечить отсутствие возможности просмотра третьими лицами.
  8. При завершении работы на персональном компьютере, работнику необходимо выключить компьютер, введя специальный ключ блокировки или эквивалентного средства контроля.
  9. Сотрудники Общества должны быть информированы об угрозах нарушения безопасности, и расписаться об этом в соответствующем документе при принятии на работу.
  10. Сотрудники обязаны без промедления сообщать о всех наблюдаемых и подозрительных вариантов нарушения правил Общества, которые могут повлечь за собой любой ущерб Обществу.

# Организационная основа деятельности по обеспечению информационной безопасности

Меры по обеспечению безопасности подразделяют на четыре вида, такие как:

* Правовые (законодательные)
* Морально-этические
* Организационные (административные)
* Физические
* Технические (аппаратные и программные)

К правовым мерам относятся действующие в РФ законы, указы и нормативные акты, регламентирующие правила работы с информацией. Правовые меры носят в основном профилактический характер и требуют постоянной разъяснительной работы с пользователем.

Морально – этические меры защиты - традиционно сложившиеся в стране нормы поведения и правила обращения с информацией. Эти нормы не являются обязательными, как законодательно утвержденные нормы, их несоблюдение ведет к падению авторитета, престижа человека, организации. Так же форма этих мер защиты может являться как формальной, так и неформальной.

Организационные (административные) – это меры, регламентирующие процессы функционирования софта пользователя, использование ее ресурсов, деятельности персонала, а также порядок взаимодействия пользователей системой таким образом, чтобы максимально затруднить или исключить возможность реализации угроз безопасности информации.

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

Все работники Общества, допущенные к работе (пользователи) и обслуживающий персонал АС, должны нести персональную ответственность за нарушения установленного порядка автоматизированной обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов АС. Каждый работник (при приеме на работу) должен подписывать «Договор о неразглашении конфиденциальной информации», а также ознакомиться с «Инструкцией о порядке работы с конфиденциальной информацией в АС».

Физические меры защиты – мера защита территории и прилегающих к ней зданий, сооружении Общества, путем установления контрольно-пропускного пункта при входе на территорию Общества, организация постов охраны, отсутствие посторонних людей в помещениях. В физические меры защиты также включены и средства ночного видения, видеокамер.

Технические меры защиты – различные электронные устройства и специальные программы, выполняющие (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию пользователей, разграничение доступа к ресурсам, криптографическое закрытие информации и т.п.)

# Ответственность за соблюдение положений Политики

Общее руководство обеспечением информационной безопасности Общества осуществляется членом руководства.

Так же за ним прикрепляется обязанность поддержания настоящей Политики в актуальном состоянии, создание, внедрение, а также координация и внесение изменений в процессы системы менеджмента информационной безопасности Общества.

Ответственность работников Общества за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с сотрудниками Общества, а также положениями внутренних нормативных документов Общества

# Контроль за соблюдением положений Политики

Общий контроль состояния информационной безопасности Общества осуществляется членом руководства.

Текущий контроль соблюдения настоящей Политики осуществляет штаб Руководства. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности Общества, по результатам оценки информационной безопасности.

# Заключительные положения

* 1. Невыполнение сотрудниками Общества требований по обеспечению ИБ приравнивается к невыполнению должностных обязанностей и приводит, как минимум, к дисциплинарной ответственности;
  2. Изменение настоящей Политики предусмотрено не реже одного раза за два календарных года;
  3. Изменения в настоящей Политике в праве вносить только назначенный член руководства;
  4. Политика в праве быть признанной недействующей только в случае принятия соответствующего решения главы отдела Безопасности вместе с главой руководства;