|  |
| --- |
| Приложение 10  к Приказу  от 07.11.2016 №33-ОД |

политика

информационной безопасности

1. Перечень используемых определений
   1. Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
   2. Администратор информационной безопасности – специалист или группа специалистов предприятия, осуществляющих контроль за обеспечением защиты информации в локальной вычислительной сети, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления несанкционированного доступа к защищаемой информации.
   3. Доступ к информации – возможность получения информации и ее использования.
   4. Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
   5. Информация – сведения (сообщения, данные) независимо от формы их представления.
   6. Информационные активы – информационные системы, информационные средства, информационные ресурсы.
   7. Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации, состояние защищенности информационных активов в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов.
   8. Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений МУП «Центртранс» г.Барнаула.
   9. Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.
   10. Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.
   11. Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.
   12. Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством РФ.
   13. Конфиденциальность – доступ к информации только авторизованных пользователей.
   14. Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений МУП «Центртранс» г.Барнаула или иного вида ущерба.
   15. Локальная вычислительная сеть – группа электронно-вычислительных машин, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.
   16. Межсетевой экран – программно-аппаратный комплекс, используемый для контроля доступа между локальными вычислительными сетями, входящими в состав сети, а также между сетью МУП «Центртранс» г.Барнаула и внешними сетями (сетью Интернет).
   17. Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.
   18. Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в МУП «Центртранс» г.Барнаула для обеспечения его информационной безопасности.
   19. Пользователь локальной вычислительной сети – сотрудник предприятия (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.
   20. Программное обеспечение – совокупность прикладных программ, установленных на сервере или электронно-вычислительной машине.
   21. Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.
   22. Регистрационная (учетная) запись пользователя включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.
   23. Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.
   24. Ответственный за техническое обеспечение – сотрудник организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети МУП «Центртранс» г.Барнаула и персонального компьютера.
   25. 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.
   26. Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности при реализации угроз в информационной сфере.
   27. Целостность информации – состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.
   28. Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
2. Вводные положения
   1. Введение

2.1.1. Политика информационной безопасности МУП «Центртранс» г.Барнаула определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется сотрудники МУП «Центртранс» г.Барнаула в своей деятельности.

* 1. Цели

2.2.1. Основными целями политики информационной безопасности являются защита информации МУП «Центртранс» г.Барнаула от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Уставе МУП «Центртранс» г.Барнаула.

2.2.2. Общее руководство обеспечением информационной безопасности осуществляется руководителем МУП «Центртранс» г.Барнаула. Ответственность за организацию мероприятий по обеспечению информационной безопасности и контроль за соблюдением требований информационной безопасности несет администратор информационной безопасности. Ответственность за функционирование информационных систем МУП «Центртранс» г.Барнаула несет администратор информационной системы.

2.2.3. Должностные обязанности администратора информационной безопасности утверждены в Регламенте ответственного за обеспечение безопасности информации в информационных системах.

2.2.4. Должностные обязанности системного администратора утверждены в Регламенте администратора информационных систем.

2.2.5. Руководители структурных подразделений МУП «Центртранс» г.Барнаула ответственны за обеспечение выполнения требований информационной безопасности в своих подразделениях.

2.2.6. Сотрудники МУП «Центртранс» г.Барнаула обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других внутренних документов МУП «Центртранс» г.Барнаула по вопросам обеспечения информационной безопасности.

* 1. Задачи

2.3.1. Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

2.3.2. Наибольшими возможностями для нанесения ущерба МУП «Центртранс» г.Барнаула обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом, при этом злоумышленник может иметь сообщников как внутри, так и вне МУП «Центртранс» г.Барнаула, либо иметь непреднамеренный ошибочный характер. Категории нарушителей и их возможности определяются в Модели нарушителя.

2.3.3. На основе вероятностной оценки определяется перечень актуальных угроз безопасности, который отражается в Модели угроз.

2.3.4. Для противодействия угрозам информационной безопасности в МУП «Центртранс» г.Барнаула составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения информационной безопасности при минимальных ресурсных затратах.

2.3.5. Разработанная на основе прогноза политика информационной безопасности и в соответствии с ней построенная система управления информационной безопасностью является наиболее правильным и эффективным способом добиться минимизации рисков нарушения информационной безопасности для МУП «Центртранс» г.Барнаула. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

2.3.6. Стратегия обеспечения информационной безопасности заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

2.3.7. Задачами настоящей политики являются:

* описание организации системы управления информационной безопасностью;
* определение Политик информационной безопасности, а именно: политика реализации антивирусной защиты; политика учетных записей; политика предоставления доступа к информационным ресурсам; политика использования паролей; политика защиты автоматизированного рабочего места; политика конфиденциального делопроизводства;
* определение порядка сопровождения информационной системы МУП «Центртранс» г.Барнаула.
  1. Область действия

2.4.1. Настоящая Политика распространяется на все структурные подразделения МУП «Центртранс» г.Барнаула и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

* 1. Период действия и порядок внесения изменений

2.5.3. Изменения, в политику вносятся приказом руководителя МУП «Центртранс» г.Барнаула.

2.5.4. Инициаторами внесения изменений в политику информационной безопасности являются:

* руководитель МУП «Центртранс» г.Барнаула;
* заместители руководителя;
* администратор информационной безопасности.

2.5.5. Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

2.5.6. Внеплановая актуализация политики информационной безопасности производится в обязательном порядке в следующих случаях:

* при изменении политики Российской Федерации в области информационной безопасности, указов и законов Российской Федерации в области защиты информации;
* при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности МУП «Центртранс» г.Барнаула;
* при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб МУП «Центртранс» г.Барнаула.

2.5.7. Ответственными за актуализацию политики информационной безопасности (плановую и внеплановую) несет администратор информационной безопасности.

2.5.8. Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на администратора информационной безопасности.

1. Политики информационной безопасности
   1. Назначение политик информационной безопасности

3.1.1. Политики информационной безопасности МУП «Центртранс» г.Барнаула – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в МУП «Центртранс» г.Барнаула.

3.1.2. Политики информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию МУП «Центртранс» г.Барнаула в области информационной безопасности.

3.1.3. Политики информационной безопасности регламентируют эффективную работу средств защиты информации. Они охватывают все особенности процесса обработки информации, определяя поведение информационной системы и ее пользователей в различных ситуациях. Политики информационной безопасности реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

* 1. Основные принципы обеспечения информационной безопасности

3.2.1. Основными принципами обеспечения информационной безопасности являются:

* постоянный и всесторонний анализ информационного пространства МУП «Центртранс» г.Барнаула с целью выявления уязвимостей информационных активов;
* своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность МУП «Центртранс» г.Барнаула, корректировка моделей угроз и нарушителя;
* разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения информационной безопасности, не должны усложнять достижение уставных целей МУП «Центртранс» г.Барнаула, а также повышать трудоемкость технологических процессов обработки информации;
* контроль эффективности принимаемых защитных мер;
* адекватное разделение ролей и ответственности между сотрудниками МУП «Центртранс» г.Барнаула, исходя из принципа персональной и единоличной ответственности за совершаемые операции.
  1. Соответствие Политики безопасности   
     действующему законодательству РФ

3.3.1. Правовую основу политик составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

* 1. Ответственность за реализацию   
     политик информационной безопасности

3.4.1. Ответственность за разработку мер и контроль обеспечения защиты информации несёт администратор информационной безопасности.

3.4.2. Ответственность за реализацию политик возлагается:

* в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты, доведения правил политик до сотрудников МУП «Центртранс» г.Барнаула, а также иных лиц– на администратора информационной безопасности;
* в части, касающейся исполнения правил политики, – на каждого сотрудника МУП «Центртранс» г.Барнаула, попадающих под область действия настоящей политики.
  1. Порядок подготовки персонала по вопросам   
     информационной безопасности и допуска его к работе

3.5.1. Организация обучения сотрудников МУП «Центртранс» г.Барнаула в области информационной безопасности возлагается на администратора информационной безопасности. Обучение проводится согласно Плану, утвержденному руководителем МУП «Центртранс» г.Барнаула.

3.5.2. Подписи сотрудников об ознакомлении заносятся в Журнал проведения инструктажа по информационной безопасности.

3.5.3. Допуск персонала к работе с защищаемыми информационными ресурсами МУП «Центртранс» г.Барнаула осуществляется только после его ознакомления с настоящими политиками, а также после ознакомления пользователей с Порядком работы пользователей МУП «Центртранс» г.Барнаула, а также иными инструкциями пользователей отдельных информационных систем. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в Журнале проведения инструктажа по информационной безопасности.

3.5.4. Допуск персонала к работе с конфиденциальной информацией МУП «Центртранс» г.Барнаула осуществляется после ознакомления с Порядком организации работы с материальными носителями, Порядок организации работы с электронными носителями. Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками МУП «Центртранс» г.Барнаула, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

* 1. Защищаемые информационные ресурсы

3.6.1. Защищаемые информационные ресурсы определяются в соответствии с Перечнем защищаемых ресурсов.

1. Политики информационной безопасности
   1. Политика предоставления доступа к информационному ресурсу

4.1.1. Настоящая Политика определяет основные правила предоставления сотрудникам МУП «Центртранс» г.Барнаула доступа к защищаемым информационным ресурсам.

4.1.2. Положения данной политики определены в Положении о разрешительной системе допуска.

* 1. Политика учетных записей

4.2.1. Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов МУП «Центртранс» г.Барнаула.

4.2.2. Регистрационные учетные записи подразделяются:

* пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов МУП «Центртранс» г.Барнаула;
* системные – используемые для нужд операционной системы;
* служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

4.2.3. Каждому пользователю информационных активов МУП «Центртранс» г.Барнаула назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

4.2.4. Запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство). Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

4.2.5. Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

4.2.6. Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

4.2.7. Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

4.2.8. Настоящая Политика определяет основные правила парольной защиты в МУП «Центртранс» г.Барнаула.

4.2.9. Положения политики закрепляются в Порядке по организации парольной защиты.

* 1. Политика реализации антивирусной защиты

4.3.1. Настоящая Политика определяет основные правила для реализации антивирусной защиты в МУП «Центртранс» г.Барнаула.

4.3.2. Положения политики закрепляются в Порядке по проведению антивирусного контроля.

* 1. Политика защиты автоматизированного рабочего места

4.4.1. Настоящая Политика определяет основные правила и требования по защите автоматизированных рабочих мест МУП «Центртранс» г.Барнаула.

* + 1. Положения политики закрепляются в Порядке организации и проведения работ по защите информации в информационных системах.
  1. Политика использования паролей

4.5.1. Настоящая Политика определяет основные правила и требования по защите информации МУП «Центртранс» г.Барнаула от неавторизованного доступа, утраты или модификации.

4.5.2. Положения данной политики определяются в Порядке организации парольной защиты в информационных системах.

5. Профилактика нарушений политик   
информационной безопасности

5.1. Под профилактикой нарушений политик информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в МУП «Центртранс» г.Барнаула и проведение разъяснительной работы по информационной безопасности среди пользователей.

5.2. Положения определены приложениями, утвержденными приказом МУП «Центртранс» г.Барнаула «Об обучении сотрудников правилам защиты информации».

6. Ликвидация последствий нарушения   
политик информационной безопасности

6.1. Администратор информационной безопасности, используя данные, полученные в результате применения средств контроля (мониторинга) безопасности информации информационной системы, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления несанкционированного доступа к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

6.2. В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления несанкционированного доступа к защищаемым информационным ресурсам информационной системы рекомендуется уведомить администратора информационной безопасности, и далее следовать их указаниям.

6.3. Действия администратора информационной безопасности и администратора информационной системы при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

6.3.1. Регламентом пользователя.

6.3.2. Политикой информационной безопасности.

6.3.3. Регламентом администратора информационной безопасности.

6.3.4. Регламентом системного администратора.

6.4. После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности информационной системы, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

7. Ответственность за нарушение   
политик безопасности

7.1. Ответственность за выполнение правил политики безопасности несет каждый сотрудник МУП «Центртранс» г.Барнаула в рамках своих служебных обязанностей и полномочий.

7.2. На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования Политики безопасности МУП «Центртранс» г.Барнаула, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

7.3. Все сотрудники несут персональную, в том числе материальную, ответственность за прямой действительный ущерб, причиненный МУП «Центртранс» г.Барнаула в результате нарушения ими правил политики информационной безопасности (ст. 238 Трудового кодекса РФ).

7.4. За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации электронно-вычислительных машин, следствием которых явилось нарушение работы электронно-вычислительной машины (автоматизированной системы обработки информации), уничтожение, блокирование или модификацию защищаемой информации, сотрудники МУП «Центртранс» г.Барнаула несут ответственность в соответствии со ст. 272, 273 и 274 Уголовного кодекса РФ.