

ПОЛИТИКА
информационной безопасности ООО "Барнаульский водоканал"

1. Общие положения

Политика ИБ Общества с ограниченной ответственностью "Барнаульский водоканал" (далее – ООО "Барнаульский водоканал") определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется ООО "Барнаульский водоканал" в своей деятельности.

2. Перечень используемых определений, обозначений и сокращений

АИБ – Администратор информационной безопасности.

АРМ – Автоматизированное рабочее место.

АС – Автоматизированная система.

ИБ – Информационная безопасность.

ИР – Информационные ресурсы.

ИС – Информационная система.

МЭ – Межсетевой экран.

ЛВС — Локальная вычислительная сеть.

НСД – Несанкционированный доступ.

ОС – Операционная система.

ПБ – Политики безопасности.

ПДн – Персональные данные.

ПО – Программное обеспечение.

СЗИ – Средство защиты информации.

СУИБ — Система управления информационной безопасностью.

ЭВМ – Электронная – вычислительная машина, персональный компьютер.

Автоматизированная система – 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.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества 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 общества.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений ООО "Барнаульский водоканал".

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

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.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений ООО "Барнаульский водоканал" или иного вида ущерба.

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.

Межсетевой экран – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью ООО "Барнаульский водоканал" и внешними сетями (сетью Интернет).

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

Политика информационной безопасности – комплекс взаимосвязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в ООО "Барнаульский водоканал" 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.

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

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

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.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Ответственный за техническое обеспечение – сотрудник организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети ООО "Барнаульский водоканал".

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.

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

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

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.

3. Вводные положения

3.1. Цели

Основными целями политики ИБ являются защита информации ООО "Барнаульский водоканал" 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 Положении о деятельности ООО "Барнаульский водоканал".

Общее руководство обеспечением ИБ осуществляется Генерального директора ООО "Барнаульский водоканал". Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет АИБ. Ответственность за функционирование информационных систем ООО "Барнаульский водоканал" несет администратор информационной системы.

Должностные обязанности АИБа и системного администратора закрепляются в соответствующих инструкциях.

Руководители структурных подразделений ООО "Барнаульский водоканал" ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники ООО "Барнаульский водоканал" обязаны соблюдать порядок обращения с конфиденциальными (содержащими персональные данные) документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов внутренних документов ООО "Барнаульский водоканал" по вопросам обеспечения ИБ.

3.2. Задачи

Политика ИБ 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.

Наибольшими возможностями для нанесения ущерба ООО "Барнаульский водоканал" обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне ООО "Барнаульский водоканал"), либо иметь непреднамеренный ошибочный характер.

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

Для противодействия угрозам ИБ в ООО "Барнаульский водоканал" на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная СУИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для ООО "Барнаульский водоканал". Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ 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.

Задачами настоящей политики являются:

- описание организации СУИБ;
- определение порядка сопровождения ИС ООО "Барнаульский водоканал".

Настоящая Политика распространяется на все структурные подразделения ООО "Барнаульский водоканал" 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.

Настоящая Политика вводится в действие Приказом Генерального директора ООО "Барнаульский водоканал".

Политика признается утратившей силу на основании Приказа Генерального директора ООО "Барнаульский водоканал".

- определение Политики ИБ, а именно: политика реализации антивирусной защиты; политика учетных записей; политика предоставления доступа к ИР; политика использования паролей; политика защиты АРМ; политика конфиденциального делопроизводства;

3.3. Область действия

3.4. Период действия и порядок внесения изменений

Изменения в политику вносятся Приказом Генерального директора ООО "Барнаульский водоканал". Инициаторами внесения изменений в политику информационной безопасности являются:

- Генеральный директор ООО "Барнаульский водоканал";
- руководители отделов ООО "Барнаульский водоканал";
- администратор информационной безопасности.

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

Внеплановая актуализация политики ИБ и производится в обязательном порядке в следующих случаях:

- при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ ООО "Барнаульский водоканал";
- при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб ООО "Барнаульский водоканал".

Ответственными за актуализацию политики ИБ (плановую и внеплановую) несет АИБ.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на АИБа.

4. Политика информационной безопасности ООО "Барнаулский водоканал"

4.1. Назначение политики информационной безопасности

Политика ИБ ООО "Барнаулский водоканал" – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в ООО "Барнаулский водоканал".

Политика ИБ относится к административным мерам обеспечения ИБ и определяют стратегию ООО "Барнаулский водоканал" в области ИБ.

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

Все документально оформленные решения, формирующие Политику, должны быть утверждены ООО "Барнаулский водоканал".

4.2. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

- постоянный и всесторонний анализ информационного пространства ООО "Барнаулский водоканал" с целью выявления уязвимостей информационных активов;
- своевременное обнаружение проблем, потенциально способных повлиять на ИБ ООО "Барнаулский водоканал", 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 ИБ, не должны усложнять достижение уставных целей ООО "Барнаулский водоканал", а также повышать трудоемкость технологических процессов обработки информации;
- контроль эффективности принимаемых защитных мер;
- персонификация и адекватное разделение ролей и ответственности между сотрудниками ООО "Барнаулский водоканал", исходя из принципа персональной и единоличной ответственности за совершаемые операции.

4.3. Соответствие Политики безопасности действующему законодательству

Правовую основу политики 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.

4.4. Ответственность за реализацию политики информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт АИБ.

Ответственность за реализацию политики возлагается:

- в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на АИБа;
- в части, касающейся доведения правил политики до сотрудников ООО "Барнаульский водоканал", а также иных лиц (см. область действия настоящей политики) – на АИБа;
- в части, касающейся исполнения правил политики, – на каждого сотрудника ООО "Барнаульский водоканал", согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

4.5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация обучения сотрудников ООО "Барнаульский водоканал" в области ИБ возлагается на АИБа. Обучение проводится согласно Плану, утвержденному Генерального директора ООО "Барнаульский водоканал".

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

Допуск персонала к работе с защищаемыми ИР ООО "Барнаульский водоканал" осуществляется только после его ознакомления с настоящей политикой, а также после ознакомления пользователей с «Порядком работы пользователей» ООО "Барнаульский водоканал", а так же иными инструкциями пользователей

отдельных ИС. Согласие на соблюдение правил и требований настоящей политики подтверждается подписями сотрудников в журналах ознакомления.

Допуск персонала к работе с ПДн ООО "Барнаульский водоканал" осуществляется после ознакомления с необходимыми организационно-распорядительными документами организации. Правила допуска к работе с ИР лиц, не являющихся сотрудниками ООО "Барнаульский водоканал", определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

4.6. Защищаемые информационные ресурсы ООО "Барнаульский водоканал"

Защищаемые информационные ресурсы определяются в соответствии с «Перечнем защищаемых ресурсов», утверждаемым соответствующим Приказом ООО "Барнаульский водоканал".

5. Политика информационной безопасности

5.1. Политика предоставления доступа к информационному ресурсу

5.1.1. Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым ИР ООО "Барнаульский водоканал".

Положения данной политики определены в «Положении о разрешительной системе допуска», утверждаемом соответствующим Приказом ООО "Барнаульский водоканал".

5.2. Политика учетных записей

5.2.1. Назначение

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов ООО "Барнаульский водоканал".

5.2.2. Положение политики

Регистрационные учетные записи подразделяются на:

– пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов ООО "Барнаульский водоканал";

– системные – используемые для нужд операционной системы;

– служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов ООО "Барнаульский водоканал" назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае 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), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

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

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

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

5.3. Политика использования паролей

5.3.1. Назначение

Настоящая Политика определяет основные правила парольной защиты в ООО "Барнаульский водоканал".

5.3.2. Положения политики

Положения политики закрепляются в «Порядке по организации парольной защиты».

5.4. Политика реализации антивирусной защиты

5.4.1. Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты в ООО "Барнаульский водоканал".

5.4.2. Положения политики

Положения политики закрепляются в «Порядке по проведению антивирусного контроля».

5.5. Политика защиты автоматизированного рабочего места

5.5.1. Назначение

Настоящая Политика определяет основные правила и требования по защите информации ООО "Барнаульский водоканал" от неавторизованного доступа, утраты или модификации.

5.5.2. Положения политики

Положения данной политики определяются в соответствии с используемым техническим решением.

6. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в ООО "Барнаульский водоканал" и проведение разъяснительной работы по ИБ среди пользователей.

Положения определены документами, утвержденными Приказом «Об обучении сотрудников правилам защиты информации», и «Порядком технического обслуживания средств вычислительной техники».

6.1. Ликвидация последствий нарушения политик информационной безопасности

АИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР ИС рекомендуется уведомить АИБа, и далее следовать их указаниям.

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

- регламентом пользователя;
- политикой информационной безопасности;
- регламентом администратора информационной безопасности;
- регламентом системного администратора.

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

6.2. Ответственность за нарушение Политик безопасности

Ответственность за выполнение правил ПБ несет каждый сотрудник ООО "Барнаульский водоканал" в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования ПБ ООО "Барнаульский водоканал", могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный ООО "Барнаульский водоканал" в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса Российской Федерации).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники ООО "Барнаульский

водоканал" несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.