Приложение 10
к Приказу
от 17.06.2024 № 112/1

ПОЛИТИКА
информационной безопасности АО «Барнаульский ВРЗ"

1. Перечень используемых определений, обозначений и сокращений.

АИБ – администратор информационной безопасности.

АРМ – автоматизированное рабочее место.

АС – автоматизированная система.

ИБ – информационная безопасность.

ИР – информационные ресурсы.

КИ – конфиденциальная информация.

ИС – информационная система.

НСД – несанкционированный доступ.

ОС – операционная система.

ПБ – политики безопасности.

СЗИ – средство защиты информации.

ЭВМ – электронная – вычислительная машина, персональный компьютер.

СУИБ – система управления информационной безопасностью.

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

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

Доступ к информации – возможность получения информации и её 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 общества, 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 АО «Барнаульский ВРЗ".

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 её 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.

Конфиденциальность – доступ к информации только авторизованных пользователей.

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

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 АО «Барнаульский ВРЗ" 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 АО «Барнаульский ВРЗ" и ПК.

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 Общества при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на неё 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.

2. Вводные положения.

2.1. Введение.

Политика ИБ Акционерного общества "Барнаульский вагоноремонтный завод" (далее – АО «Барнаульский ВРЗ") определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется АО «Барнаульский ВРЗ" в своей деятельности.

2.2. Цели.

Основными целями политики ИБ являются защита информации АО «Барнаульский ВРЗ" от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Положение АО «Барнаульский ВРЗ".

Общее руководство обеспечением ИБ осуществляется Генеральным директором АО «Барнаульский ВРЗ". Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет АИБ. Ответственность за функционирование информационных систем АО «Барнаульский ВРЗ" несет администратор информационной системы (далее – администратор ИС).

Должностные обязанности АИБа и администратора ИС закрепляются в соответствующих инструкциях.

Руководители структурных подразделений АО «Барнаульский ВРЗ" ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники АО «Барнаульский ВРЗ" обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других внутренних документов АО «Барнаульский ВРЗ" по вопросам обеспечения ИБ.

2.3. Задачи.

Обработка КИ в АО «Барнаульский ВРЗ" осуществляется для решения следующих задач:

— ведение кадрового и бухгалтерского учета;

- исполнение судебного акта;
- обеспечение соблюдения пенсионного законодательства РФ;
- обеспечение пропускного режима на территорию оператора;
- обеспечение соблюдения налогового законодательства РФ;
- обеспечение соблюдения страхового законодательства РФ;
- подготовка, заключение и исполнение гражданско-правового договора;
- обеспечение соблюдения трудового законодательства РФ;
- обеспечение соблюдения законодательства РФ о связи.
- обеспечение законов и иных форм нормативно-правовых актов в отношении работников Общества, содействия работникам в обучении и продвижении по работе, обеспечении личной безопасности работников, соблюдение основных государственных гарантий по оплате труда работников контроля количества и качества выполняемой работы;

Политика ИБ направлена на защиту информационных активов, в том числе ПДн, 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 АО «Барнаульский ВРЗ" обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне АО «Барнаульский ВРЗ"), либо иметь непреднамеренный ошибочный характер. Категории нарушителей и их возможности определяются в «Модели нарушителя».

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

Для противодействия угрозам ИБ в АО «Барнаульский ВРЗ" 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 АО «Барнаульский ВРЗ". 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, в том числе ИСПДн (далее – ИС) АО «Барнаульский ВРЗ".

— 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.

2.4. Область действия.

Настоящая Политика распространяется на все структурные подразделения АО «Барнаульский ВРЗ" 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.

2.5. Период действия и порядок внесения изменений.

Настоящая Политика вводится в действие Приказом Генерального директора АО «Барнаульский ВРЗ".

Политика признается утратившей силу на основании Приказа Генерального директора АО «Барнаульский ВРЗ".

Изменения в политику вносятся Приказом Генерального директора АО «Барнаульский ВРЗ".

Инициаторами внесения изменений в политику информационной безопасности являются:

— генеральный директор АО «Барнаульский ВРЗ";

— руководители подразделений АО «Барнаульский ВРЗ";

— АИБ.

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 производится в обязательном порядке в следующих случаях:

— при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ АО «Барнаульский ВРЗ";

— при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб АО «Барнаульский ВРЗ"

— при изменении политики Российской Федерации в области ИБ, указов и законов Российской Федерации в области защиты информации.

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

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

3. Политика информационной безопасности АО «Барнаульский ВРЗ".

3.1. Назначение политики информационной безопасности.

Политики ИБ АО «Барнаульский ВРЗ" – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в АО «Барнаульский ВРЗ".

Политики ИБ относятся к административным мерам обеспечения ИБ и определяют стратегию АО «Барнаульский ВРЗ" в области ИБ.

Политики ИБ регламентируют эффективную работу СЗИ. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и её 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 Генеральным директором АО «Барнаульский ВРЗ".

3.2. Основные принципы обеспечения информационной безопасности.

Основными принципами обеспечения ИБ являются следующие:

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

3.3. Соответствие Политики безопасности действующему законодательству.

Правовую основу политики составляют следующие нормативные правовые акты Российской Федерации:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» 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.

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

3.4. Ответственность за реализацию политики информационной безопасности.

Ответственность за реализацию политик информационной безопасности 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 АО «Барнаульский ВРЗ", а также иных лиц (см. область действия настоящей политики) – на АИБа;
- в части, касающейся исполнения правил политики, – на каждого сотрудника АО «Барнаульский ВРЗ", согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

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

Организация обучения сотрудников АО «Барнаульский ВРЗ" в области ИБ возлагается на АИБа. Обучение проводится согласно плану, утвержденному Генерального директора АО «Барнаульский ВРЗ".

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

Допуск персонала к работе с защищаемыми ИР АО «Барнаульский ВРЗ" осуществляется только после его ознакомления с настоящими политиками, а также после ознакомления пользователей с «Инструкцией по работе пользователей в информационных системах АО «Барнаульский ВРЗ"», а так же иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Допуск персонала к работе с КИ АО «Барнаульский ВРЗ" осуществляется после ознакомления с «Инструкцией по организации работы с материальными носителями», «Инструкцией по организации работы с электронными носителями». Правила допуска к работе с ИР лиц, не являющихся сотрудниками АО «Барнаульский ВРЗ", определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

3.6. Защищаемые информационные ресурсы АО «Барнаульский ВРЗ".

Защищаемые информационные ресурсы определяются в соответствии с «Перечнем защищаемых ресурсов», утверждаемым соответствующим Приказом Генеральным директором АО «Барнаульский ВРЗ".

4. Политики информационной безопасности.

4.1. Политика предоставления доступа к информационному ресурсу.

4.1.1. Назначение.

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым ИР АО «Барнаульский ВРЗ".

4.1.2. Положение политики.

Положения данной политики определены в «Положении о разрешительной системе допуска», утверждаемом соответствующим Приказом Генеральным директором АО «Барнаульский ВРЗ".

4.2. Политика учетных записей.

4.2.1. Назначение.

Настоящая политика определяет основные правила присвоения учетных записей пользователям ИС АО «Барнаульский ВРЗ".

4.2.2. Положение политики.

Регистрационные учетные записи подразделяются на:

— пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов АО «Барнаульский ВРЗ";

— системные – используемые для нужд операционной системы;

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

Каждому пользователю информационных активов АО «Барнаульский ВРЗ" 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.

4.3. Политика реализации антивирусной защиты.

4.3.1. Назначение.

Настоящая Политика определяет основные правила для реализации антивирусной защиты в АО «Барнаульский ВРЗ".

4.3.2. Положения политики.

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

4.4. Политика защиты автоматизированного рабочего места.

4.4.1. Назначение.

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

4.4.2. Положения политики.

Положения данной политики определяются в соответствии с используемым техническим решением.

4.5. Политика использования паролей.

4.5.1. Назначение.

Настоящая Политика определяет основные правила парольной защиты в АО «Барнаульский ВРЗ".

4.5.2. Положения политики.

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

5. Профилактика нарушений политик информационной безопасности.

Под профилактикой нарушений политик ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в АО «Барнаульский ВРЗ" 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».

5.1. 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 его указаниям.

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

5.1.1. регламентом пользователя;

5.1.2. политикой информационной безопасности;

5.1.3. регламентом АИБа;

5.1.4. регламентом администратора ИС.

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.

5.2. Ответственность за нарушение Политик безопасности

Ответственность за выполнение правил ПБ несет каждый сотрудник АО «Барнаульский ВРЗ" в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования ПБ АО «Барнаульский ВРЗ", 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 АО «Барнаульский ВРЗ" 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 АО «Барнаульский ВРЗ" несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.