Приложение 10
к Приказу «Об организации работы по защите конфиденциальной информации и персональных данных»
от 28.04.2021 № 12

Нестерова Наталья Валентиновна
Подписано цифровой подписью: Нестерова Наталья Валентиновна
Дата: 2021.06.09 13:01:56 +07'00'

ПОЛИТИКА
информационной безопасности МБДОУ ЦРР - "Детский сад № 217"

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.
КИ — Конфиденциальная информация.
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 МБДОУ ЦРР - «Детский сад № 217».

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.

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 МБДОУ ЦРР - «Детский сад № 217» 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 МБДОУ ЦРР - «Детский сад № 217» и внешними сетями (сетью Интернет).

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 МБДОУ ЦРР - «Детский сад № 217» 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 МБДОУ ЦРР - «Детский сад № 217».

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, характеризуемое способностью АС обеспечивать сохранность и неизменность

конфиденциальной информации 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.

1. **Вводные положения**

1.1. **Введение**

Политика ИБ Муниципального бюджетного дошкольного образовательного учреждения центр развития ребенка - «Детский сад № 217» (далее - МБДОУ ЦРР - «Детский сад № 217») определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется МБДОУ ЦРР - «Детский сад № 217» в своей деятельности.

1.2. **Ц е л и**

Основными целями политики ИБ являются защита информации МБДОУ ЦРР - «Детский сад № 217» 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 МБДОУ ЦРР - «Детский сад № 217».

Общее руководство обеспечением ИБ осуществляется заведующим МБДОУ ЦРР - «Детский сад № 217». Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет АИБ. Ответственность за функционирование информационных систем МБДОУ ЦРР - «Детский сад № 217» несет администратор информационной системы.

Должностные обязанности АИБа и системного администратора закрепляются в соответствующих инструкциях.

Руководители структурных подразделений МБДОУ ЦРР - «Детский сад № 217» ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники МБДОУ ЦРР - «Детский сад № 217» обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и

других документов внутренних документов МБДОУ ЦРР - «Детский сад № 217» по вопросам обеспечения ИБ.

1.3. **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 МБДОУ ЦРР - «Детский сад № 217» обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне МБДОУ ЦРР - «Детский сад № 217»), либо иметь непреднамеренный ошибочный характер.

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

Для противодействия угрозам ИБ в МБДОУ ЦРР - «Детский сад № 217» 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 МБДОУ ЦРР - «Детский сад № 217». 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 МБДОУ ЦРР - «Детский сад № 217».

Настоящая Политика распространяется на все структурные подразделения МБДОУ ЦРР - «Детский сад № 217» 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 заведующего МБДОУ ЦРР - «Детский сад № 217».

Политика признается утратившей силу на основании Приказа заведующего МБДОУ ЦРР - «Детский сад № 217».

– 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;

1.4. **Область действия**

Период действия и порядок внесения изменений

Изменения в политику вносятся Приказом заведующего МБДОУ ЦРР - «Детский сад № 217». Инициаторами внесения изменений в политику информационной безопасности являются:

– заведующий МБДОУ ЦРР - «Детский сад № 217»;

– руководители структурных подразделений МБДОУ ЦРР - «Детский сад № 217»;

– администратор информационной безопасности.

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

Актуализация политики ИБ производится в обязательном порядке в следующих случаях:

– при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ МБДОУ ЦРР - «Детский сад № 217»;

– при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб МБДОУ ЦРР - «Детский сад № 217».

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.

2. Политика информационной безопасности МБДОУ ЦРР - «Детский сад № 217»

2.1. Назначение политики информационной безопасности

Политика ИБ МБДОУ ЦРР - «Детский сад № 217» – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в МБДОУ ЦРР - «Детский сад № 217».

Политика ИБ относятся к административным мерам обеспечения ИБ и определяют стратегию МБДОУ ЦРР - «Детский сад № 217» 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 заведующим МБДОУ ЦРР - «Детский сад № 217».

2.2. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

– постоянный и всесторонний анализ информационного пространства МБДОУ ЦРР - «Детский сад № 217» с целью выявления уязвимостей информационных активов;

– своевременное обнаружение проблем, потенциально способных повлиять на ИБ МБДОУ ЦРР - «Детский сад № 217», 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 МБДОУ ЦРР - «Детский сад № 217», а также повышать трудоемкость технологических процессов обработки информации;

– контроль эффективности принимаемых защитных мер;

– персонификация и адекватное разделение ролей и ответственности между сотрудниками МБДОУ ЦРР - «Детский сад № 217», исходя из принципа персональной и единоличной ответственности за совершаемые операции.

2.3. **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.

2.4. **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 МБДОУ ЦРР - «Детский сад № 217», а также иных лиц (см. область действия настоящей политики) – на АИБа;

– в части, касающейся исполнения правил политики, – на каждого сотрудника МБДОУ ЦРР - «Детский сад № 217», согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

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

Организация обучения сотрудников МБДОУ ЦРР - «Детский сад № 217» в области ИБ возлагается на АИБа. Обучение проводится согласно Плану, утвержденному заведующим МБДОУ ЦРР - «Детский сад № 217».

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

Допуск персонала к работе с защищаемыми ИР МБДОУ ЦРР - «Детский сад № 217» осуществляется только после его ознакомления с настоящей политикой, а также после ознакомления пользователей с «Порядком работы пользователей» МБДОУ ЦРР - «Детский сад № 217», 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 КИ МБДОУ ЦРР - «Детский сад № 217» осуществляется после ознакомления с «Порядком организации работы с материальными носителями», «Порядком организации работы с электронными

носителями». Правила допуска к работе с ИР лиц, не являющихся сотрудниками МБДОУ ЦРР - «Детский сад № 217», определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

2.6. **Защищаемые информационные ресурсы МБДОУ ЦРР - «Детский сад № 217»**

Защищаемые информационные ресурсы определяются в соответствии с «Перечнем защищаемых ресурсов», утверждаемым соответствующим Приказом заведующего МБДОУ ЦРР - «Детский сад № 217».

3. **Политика информационной безопасности**

3.1. **Политика предоставления доступа к информационному ресурсу**

3.1.1. **Назначение**

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым ИР МБДОУ ЦРР - «Детский сад № 217».

Положения данной политики определены в «Положении о разрешительной системе допуска», утверждаемом соответствующим Приказом заведующего МБДОУ ЦРР - «Детский сад № 217».

3.2. **Политика учетных записей**

3.2.1. **Назначение**

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов МБДОУ ЦРР - «Детский сад № 217».

3.2.2. **Положение политики**

Регистрационные учетные записи подразделяются на:

– пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов МБДОУ ЦРР - «Детский сад № 217»;

– системные – используемые для нужд операционной системы;

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

Каждому пользователю информационных активов МБДОУ ЦРР - «Детский сад № 217» 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.

3.3. **Политика использования паролей**

3.3.1. **Назначение**

Настоящая Политика определяет основные правила парольной защиты в МБДОУ ЦРР - «Детский сад № 217».

3.3.2. **Положения политики**

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

3.4. **Политика реализации антивирусной защиты**

3.4.1. **Назначение**

Настоящая Политика определяет основные правила для реализации антивирусной защиты в МБДОУ ЦРР - «Детский сад № 217».

3.4.2. **Положения политики**

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

3.5. **Политика защиты автоматизированного рабочего места**

3.5.1. **Назначение**

Настоящая Политика определяет основные правила и требования по защите информации МБДОУ ЦРР - «Детский сад № 217» от неавторизованного доступа, утраты или модификации.

3.5.2. **Положения политики**

Положения данной политики определяются в соответствии с используемым техническим решением.

4. **Профилактика нарушений политик информационной безопасности**

Под профилактикой нарушений политик ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в МБДОУ ЦРР - «Детский сад № 217» 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».

4.1. **Ликвидация последствий нарушения политики 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.

4.2. **Ответственность за нарушение Политик безопасности**

Ответственность за выполнение правил ПБ несет каждый сотрудник МБДОУ ЦРР - «Детский сад № 217» в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования ПБ МБДОУ ЦРР - «Детский сад № 217», 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 МБДОУ ЦРР - «Детский сад № 217» 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 МБДОУ ЦРР - «Детский сад № 217» несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.