Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение

высшего образования

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ

МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

им. Н.П. ОГАРЁВА»

(ФГБОУ ВО «МГУ им. Н.П. Огарёва»)

Факультет математики и информационных технологий

Кафедра фундаментальной информатики

**ЛАБОРАТОРНАЯ РАБОТА №1**

по дисциплине: Системы информационной безопасности предприятия

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Автор лабораторной работы А. Е. Конышев

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Преподаватель Е. Н. Гришанов

Оценка: \_\_\_\_\_\_\_

Саранск 2023

УТВЕРЖДЕНА

Генеральным директором ЦДРиДО

«14» августа 2023 г.

(протокол №4)

Политика

информационной безопасности

Центра детского развития и дополнительного образования «Талантиум»

САРАНСК 2023**Содержание**

1. Перечень используемых определений, обозначений и сокращений……. 3

2. Вводные положения 6

2.1. Введение 6

2.2. Цели 6

2.3. Задачи 7

2.4. Область действия 8

2.5. Период действия и порядок внесения изменений 8

3. Политики информационной безопасности ЦДРиДО 9

3.1. Назначение политик информационной безопасности 9

3.2. Основные принципы обеспечения информационной безопасности 10

3.3. Соответствие Политики безопасности действующему законодательству 10

3.4. Ответственность за реализацию политик информационной безопасности 10

3.5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе 11

3.6. Защищаемые информационные ресурсы ЦДРиДО 12

4. Политики информационной безопасности 12

4.1. Политика предоставления доступа к информационному ресурсу 12

4.1.1. Назначение 12

4.1.2. Положение политики 12

4.2. Политика учетных записей 12

4.2.1. Назначение 12

4.2.2. Положение политики 12

4.3. Политика использования паролей 13

4.3.1. Назначение 13

4.3.2. Положения политики 13

5. Профилактика нарушений политик информационной безопасности 13

5.1. Ликвидация последствий нарушения политик информационной безопасности 14

5.2. Ответственность за нарушение Политик безопасности 15

**1. 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. НСД – Несанкционированный доступ.

ОС – Операционная система.

ПБ – Политики безопасности.

ПДн – Персональные данные.

ПО – Программное обеспечение.

СЗИ – Средство защиты информации.

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.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

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 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.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений предприятия или организации.

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 предприятия или организации.

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

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

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в организации 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.).

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 предприятия.

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.

**2. Вводные положения**

**2.1. Введение**

Политика информационной безопасности Центра детского развития и дополнительного образования "Талантиум" (далее Центр) определяет цели и задачи системы обеспечения информационной безопасности. Она устанавливает совокупность правил, требований и руководящих принципов, которыми руководствуется Центр в своей деятельности в области информационной безопасности. ПИБ Центра направлена на защиту конфиденциальности информации, предотвращение угроз и минимизацию рисков в этой области.

**2.2. Цели**

Основные цели ПИБ включают защиту информации Центра от возможного нанесения ущерба в виде материального, физического, морального или иного воздействия на информацию, ее носители, процессы обработки и передачи. Политика ИБ также направлена на обеспечение эффективной работы информационно-вычислительного комплекса при осуществлении деятельности, описанной в Положении о деятельности Центра.

Общее руководство по обеспечению информационной безопасности осуществляется Заведующим Центра. Администратор информационной безопасности несет ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ. Администратор информационной системы несет ответственность за функционирование информационных систем Центра.

Должностные обязанности Администратора информационной безопасности и системного администратора закреплены в соответствующих инструкциях. Сотрудники Центра обязаны соблюдать порядок обращения с конфиденциальными документами и другой защищаемой информацией, а также соблюдать требования Политики информационной безопасности и других внутренних документов Центра, связанных с обеспечением ИБ.

**2.3. Задачи**

ПИБ направлена на защиту информационных активов от угроз, вызванных противоправными действиями злоумышленников. Она также направлена на уменьшение рисков и минимизацию потенциального вреда, связанного с авариями, непреднамеренными ошибками персонала, техническими сбоями, неправильными технологическими решениями в процессах обработки, передачи и хранения информации, а также на обеспечение нормального функционирования технологических процессов.

Одним из наиболее вероятных источников угроз для Центра является внутренний персонал. Действия персонала могут быть мотивированы злым умыслом, причем злоумышленник может иметь сообщников как внутри, так и вне Центра, или же иметь непреднамеренный характер ошибочных действий.

Для противодействия угрозам информационной безопасности в Центре используется прогностическая модель, основанная на имеющемся опыте. Эта модель предполагает возможные угрозы и модель нарушителя. Чем более точен прогноз (модель угроз и модель нарушителя), тем ниже риски нарушения информационной безопасности, при этом затраты ресурсов минимальны.

Разработанная на основе прогноза политика информационной безопасности и соответствующая ей система управления информационной безопасностью являются наиболее правильным и эффективным способом минимизации рисков нарушения информационной безопасности для Центра. Важно учитывать, что с течением времени меняется характер угроз, поэтому необходимо своевременно обновлять модели угроз и нарушителя, используя данные мониторинга и аудита.

Стратегия обеспечения информационной безопасности заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, которые помогают минимизировать возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

1. описание организации СУИБ;
2. определение Политик 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. определение порядка сопровождения ИС Центра.

**2.4. Область действия**

Настоящая Политика информационной безопасности распространяется на всех сотрудников Центра и является обязательной для исполнения всеми сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах, связанных с информационной безопасностью.

**2.5. Период действия и порядок внесения изменений**

Настоящая Политика вводится в действие Приказом генерального директора Центра.

Политика признается утратившей силу на основании Приказа генерального директора Центра.

Изменения в политику вносятся Приказом генерального директора Центра.

Инициаторами внесения изменений в политику информационной безопасности являются:

1. генеральный директор Центра;
2. заведующий Центра;
3. руководители отделов Центра;
4. администратор информационной безопасности.

Плановая актуализация настоящей Политики информационной безопасности Центра производится ежегодно с целью приведения в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации. Это позволяет обеспечить актуальность и эффективность политики на протяжении времени.

В процессе актуализации Политики информационной безопасности Центра могут вноситься изменения и дополнения в соответствии с изменяющимися угрозами, требованиями законодательства и лучшими практиками в области информационной безопасности. Актуализация также может включать обновление процедур, правил и технических мер безопасности.

Целью плановой актуализации является обеспечение соответствия политики реальным условиям и повышение эффективности защиты информации Центра. Это позволяет Центру адаптироваться к изменяющимся угрозам и требованиям информационной безопасности, а также повышает осведомленность и ответственность сотрудников в области защиты информации.

Плановая актуализация настоящей Политики проводится с участием соответствующих заинтересованных сторон, таких как IT-отдел, юридический отдел и технические специалисты. Это гарантирует участие различных экспертов и обеспечивает комплексный подход к защите информации в Центре.

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

1. при изменении политики Российской Федерации в области ИБ, указов и законов Российской Федерации в области защиты информации;
2. при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ Центра;
3. при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб Центра.

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.

**3. Политики информационной безопасности ЦДРиДО**

**3.1. Назначение политик информационной безопасности**

Политики информационной безопасности Центра представляют собой совокупность норм, правил и практических рекомендаций, которые служат основой для управления, защиты и распределения информации в Центре.

Они относятся к административным мерам обеспечения информационной безопасности и определяют стратегию Центра в области информационной безопасности. Политики информационной безопасности Центра регламентируют эффективную работу систем защиты информации. Они охватывают все особенности процесса обработки информации, определяют поведение информационной системы и ее пользователей в различных ситуациях.

Политики информационной безопасности Центра реализуются с помощью административно-организационных мер, физических и программно-технических средств. Они также определяют архитектуру системы защиты информации в Центре.

Все документально оформленные решения, формирующие Политики, должны быть утверждены руководством Центра.

**3.2. Основные принципы обеспечения информационной безопасности**

Основными принципами обеспечения ИБ являются следующие:

1. анализ информационного пространства: проведение постоянного и всестороннего анализа информационного пространства Центра для выявления уязвимостей информационных активов;
2. обнаружение проблем: Своевременное обнаружение проблем, которые могут повлиять на ИБ Центра, и корректировка моделей угроз и нарушителей;
3. разработка и внедрение защитных мер: разработка и внедрение адекватных защитных мер, которые соответствуют выявленным угрозам. При этом необходимо учитывать затраты на реализацию мер и их согласование с уставными целями Центра;
4. контроль эффективности: контроль эффективности принимаемых защитных мер и постоянный мониторинг состояния информационной безопасности Центра;
5. персонификация и разделение ролей: Персонификация и адекватное разделение ролей и ответственности между сотрудниками Центра на основе принципа персональной и единоличной ответственности за совершаемые операции.

**3.3. Соответствие Политики безопасности действующему законодательству**

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.

**3.4. Ответственность за реализацию политик информационной безопасности**

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

Ответственность за реализацию политик возлагается:

1. разработка и актуализация правил внешнего доступа и управления доступом, антивирусной защиты - ответственность лежит на АИБ;
2. доведение правил политик до сотрудников Центра и других лиц - является ответственностью АИБ;
3. исполнение правил политики – каждый сотрудник Центра несет ответственность за исполнение правил политики в соответствии с их должностными и функциональными обязанностями. Также, любые другие лица, попадающие под область действия политики, также обязаны соблюдать правила политики.

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

Организация обучения сотрудников Центра в области информационной безопасности (ИБ) возлагается на АИБа. Обучение проводится в соответствии с Планом, который должен быть утвержден Заведующим Центра.

Для отслеживания ознакомления сотрудников с правилами ИБ, подписи сотрудников заносятся в "Журнал проведения инструктажа по информационной безопасности". Это позволяет иметь документированное подтверждение ознакомления каждого сотрудника с правилами и политиками ИБ.

Допуск персонала к работе с защищаемыми ИС Центра осуществляется в соответствии с определенными процедурами:

1. ознакомление с политиками: персонал должен быть ознакомлен с настоящими политиками информационной безопасности Центра, а также с "Порядком работы пользователей" и другими инструкциями, связанными с конкретными информационными системами. Согласие на соблюдение правил и требований политик подтверждается подписью сотрудников в "Журнале проведения инструктажа по информационной безопасности".
2. допуск к работе с материальными и электронными носителями: после ознакомления с "Порядком организации работы с материальными носителями" и "Порядком организации работы с электронными носителями", персонал получает допуск к работе с соответствующими информационными ресурсами.
3. допуск лиц, не являющихся сотрудниками Центра: правила допуска к работе с информационными ресурсами для таких лиц определяются на договорной основе с ними или с организациями, представителями которых они являются.

**3.6. Защищаемые информационные ресурсы ЦДРиДО**

Защищаемые информационные ресурсы Центра определяются в соответствии с "Перечнем защищаемых ресурсов". Этот перечень утверждается соответствующим Приказом Центра.

**4. Политики информационной безопасности**

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

**4.1.1. Назначение**

Назначение политики предоставления доступа к информационному ресурсу заключается в определении правил и процедур, которые регулируют предоставление доступа к защищаемым информационным ресурсам в организации.

**4.1.2. Положение политики**

Положения данной политики определены в «Положении о разрешительной системе допуска», утверждаемом соответствующим Приказом Центра.

**4.2. Политика учетных записей**

**4.2.1. Назначение**

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов Центра.

**4.2.2. Положение политики**

Регистрационные учетные записи подразделяются на:

1. пользовательские – предназначенные для идентификации или аутентификации пользователей информационных активов Центра;
2. системные – используемые для нужд операционной системы;
3. служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Пользователям информационных активов Центра детского развития и дополнительного образования (Центра) назначается уникальная пользовательская регистрационная учетная запись. Возможна привязка нескольких пользовательских учетных записей к одному пользователю, при этом учетные записи могут иметь различный уровень полномочий.

Общая пользовательская учетная запись для группы пользователей запрещена. В случаях, где необходимо использование общей учетной записи, например, для посменного дежурства или автоматизированных бизнес-процессов, должна быть отметка в журнале учета машинного времени, которая однозначно идентифицирует текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Операционная система формирует системные регистрационные учетные записи, которые следует использовать только в соответствии с документацией операционной системы. Системные учетные записи предназначены для специальных случаев, указанных в документации.

Служебные регистрационные учетные записи используются исключительно для запуска сервисов или приложений. Они предназначены для обеспечения функционирования сервисов и приложений, а не для регистрации пользователей.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено. Это правило помогает обеспечить безопасность системы и предотвратить возможные нарушения доступа и конфиденциальности.

**4.3. Политика использования паролей**

**4.3.1. Назначение**

Настоящая Политика определяет основные правила парольной защиты в Центра.

**4.3.2. Положения политики**

Для учетных записей сотрудников Центра требуется соблюдение следующих правил для паролей:

1. Длина пароля: Минимальная длина пароля должна быть не менее 12 символов.
2. Включение различных типов символов: Пароль должен содержать как заглавные, так и прописные буквы, цифры и специальные символы. Примеры специальных символов могут включать символы скобок, процента и т. д.
3. Ответственность пользователя: Пользователь, к которому привязана учетная запись, несет ответственность за соблюдение правил пароля. Если правила не соблюдаются, пользователь может нести последствия, связанные с безопасностью и доступом к информационным ресурсам.

**5. Профилактика нарушений политик информационной безопасности**

Под профилактикой нарушений политик информационной безопасности (ИБ) в Центре понимается выполнение регламентных мероприятий, направленных на защиту информации, предотвращение потенциальных нарушений ИБ и проведение информационно-образовательной работы среди пользователей.

Документы, утвержденные Приказом «Об обучении сотрудников правилам защиты информации» и «Порядком технического обслуживания средств вычислительной техники», определяют основные положения и процедуры, связанные с профилактикой нарушений, политик ИБ в Центра. Эти документы служат руководством для сотрудников и определяют правила и требования, которые должны быть соблюдены при проведении профилактических мероприятий и обслуживания компьютерного оборудования.

Проведение профилактики нарушений политик ИБ в Центре является одним из ключевых аспектов обеспечения безопасности информации и поддержания надежности систем и данных.

**5.1. Ликвидация последствий нарушения политик информационной безопасности**

АИБ должна использовать данные, полученные из инструментальных средств контроля (мониторинга) безопасности ИС, для своевременного обнаружения нарушений ИБ, фактов НСД к защищаемым информационным ресурсам и принимать меры для их локализации и устранения.

Если подсистема защиты информации обнаруживает факт нарушения ИБ или НСД к защищаемым ИР ИС, рекомендуется уведомить АИБ и следовать их указаниям. АИБ будет ответственным за координацию и принятие дальнейших мер по расследованию и реагированию на нарушения ИБ.

Обмен информацией между подсистемой защиты информации и АИБом помогает обеспечить быстрое реагирование на нарушения ИБ и минимизировать потенциальные угрозы для ИС.

Внутренние документы, регламентирующие действия АИБа и администратора информационной системы при нарушении политик информационной безопасности, включают:

1. регламент пользователя;
2. политика информационной безопасности;
3. регламент администратора информационной безопасности;
4. регламент системного администратора.

После устранения инцидента, рекомендуется выполнить следующие действия:

1. составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС. В акте следует описать суть инцидента, принятые меры для его устранения, а также результаты восстановления ИС. Это поможет документировать произошедшее и служить основой для анализа и предотвращения подобных инцидентов в будущем;
2. зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий. В этом журнале следует фиксировать все события, связанные с нарушениями ИБ, включая детали инцидента, принятые меры, результаты и даты. Регистрация в журнале позволяет отслеживать и анализировать нарушения, а также оценивать эффективность принятых мер.

**5.2. Ответственность за нарушение Политик безопасности**

Ответственность за выполнение правил ПБ несет каждый сотрудник Центра в рамках своих служебных обязанностей и полномочий.

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