

Муниципальное бюджетное учреждение дополнительного образования
«Дом детского творчества»

муниципального образования – Пригородный район Республики Северная Осетия-Алания

СОГЛАСОВАНО:

Протокол Педагогического Совета
МБУДО ДДТ

от 9.01.2019 № 3



УТВЕРЖДАЮ:

Директор МБУДО ДДТ

Волохова Л.Л.

2019г.

УТВЕРЖДЕНО:

Приказом МБУДО ДДТ

от 09.01.2019 № 1

**ПОЛОЖЕНИЕ ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ
СИСТЕМЫ АИС «СЕТЕВОЙ ГОРОД. ОБРАЗОВАНИЕ»**

1. Общие положения

- 1.1. Настоящее Положение определяет требования по обеспечению безопасности автоматизированной информационной системы (далее АИС) МБУДО ДДТ - АИС «Сетевой город. Образование».
- 1.2. АИС представляет собой IT-систему, предназначенную для автоматизации процессов формирования, обработки и анализа информации по основным направлениям деятельности ДДТ.
- 1.3. Основными функциональными возможностями АИС являются:
 - формирование, хранение и обновление сведений о ДДТ;
 - формирование, хранение и обновление сведений о педагогическом составе и сотрудниках;
 - формирование, хранение и обновление сведений об учебной нагрузке педагогического состава;
 - формирование, хранение и обновление сведений об учебно-методической продукции;
 - формирование, хранение и обновление сведений об обучающихся;
 - формирование, хранение и обновление сведений о результатах учебного процесса (итоги тестирования, экзаменов);
 - аналитическая обработка информации о проведении учебного процесса как за отчётный период, так и о текущей деятельности.
- 1.4. В качестве информации, подлежащей защите в АИС, рассматриваются:
 - персональные данные педагогического состава и сотрудников ДДТ;
 - персональные данные обучающихся;
 - персональные данные административно-хозяйственных работников.
- 1.5. При обеспечении безопасности персональных данных в информационной системе ДДТ руководствуется следующим:
 - выбор средств защиты информации для системы защиты персональных данных;
 - определение типа угроз безопасности персональных данных, актуальных для информационной системы;

- установление и обеспечение уровня защищённости персональных данных в ИС производится в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства РФ от 1 ноября 2012 г. №1119.
- 1.6. Основными группами угроз, на противостояние которым направлены цели и требования безопасности, являются:

- угрозы, связанные с осуществлением несанкционированного доступа (ознакомления) с информацией, содержащей сведения о персональных данных работников и обучающихся, при её обработке и хранении;
- угрозы, связанные с несанкционированным копированием (хищением) информации, содержащей сведения о персональных данных работников и обучающихся;
- угрозы, связанные с осуществлением доступа к информации, содержащей сведения о персональных данных работников и обучающихся, без разрешения на то ее владельца;
- (субъекта персональных данных);
- угрозы, связанные с нарушением порядка доступа к информации, содержащей сведения о персональных данных работников и обучающихся, передаваемой заинтересованным лицам;
- угрозы, связанные с перехватом информации, содержащей сведения о персональных данных работников и обучающихся, из каналов передачи данных с использованием специализированных программно-технических средств;
- угрозы, связанные с потерей (утратой) информации, содержащей сведения о персональных данных работников и обучающихся, вследствие сбоя (отказов) программного и аппаратного обеспечения;
- угрозы, связанные с внедрением компьютерных вирусов и другого вредоносного программного обеспечения;
- угрозы, связанные с осуществлением несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.).

1.7. Функциональные требования безопасности охватывают:

- требования к осуществлению аудита безопасности;
- требования к обеспечению подлинности субъектов обмена информацией;
- требования к криптографической поддержке;
- требования к защите информации, содержащей сведения о персональных данных работников и обучающихся;
- требования к идентификации и аутентификации пользователей АИС;
- требования к управлению безопасностью;
- требования к защите системы безопасности.

2. Основные функциональные возможности АИС, связанные с обеспечением безопасности (защитой информации)

2.1. Защита данных пользователя

2.2. АИС должна осуществлять функции и политику избирательного управления доступом. Избирательное управление доступом должно предоставлять возможность ограничивать и контролировать доступ к системе и к информации, содержащей сведения о персональных данных.

2.3. Каждый Пользователь, пытающийся получить доступ к АИС, сначала должен проходить процедуру идентификации и аутентификации, а затем, при попытках

пользователя до ее разблокирования администратором АИС или по истечении времени действия, заданного для счетчика блокировки.

2.15. Защита системы безопасности:

- 2.16. АИС должна предоставлять ряд возможностей для обеспечения защиты системы безопасности. Изоляция процессов и поддержания домена безопасности должны обеспечивать безопасное выполнение функций системы безопасности АИС. Возможность осуществления периодического тестирования среды функционирования АИС (аппаратной части) и собственно самих функций системы безопасности АИС должно обеспечивать поддержание уверенности администратора АИС в целостности и корректности функционирования функций системы безопасности.

3. Основные функциональные возможности повышения надежности:

- 3.1. АИС должна обеспечивать надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.
- 3.2. **Резервное копирование данных:**
- 3.3. В АИС должны входить стандартные средства предотвращения потери данных и их восстановления в случае возможных сбоев. Имеющиеся средства резервного копирования должны предоставлять Пользователям возможность выбора различных стратегий резервного копирования, обеспечивающих необходимый уровень защиты данных в случае возникновения сбоев в работе системы, при этом Пользователям должна предоставляться возможность выполнения резервного копирования данных на несъемные и съемные устройства хранения.
- 3.4. **Восстановление системы:**
- 3.5. Функциональные возможности восстановления системы должны позволять возвращать АИС в состояние, предшествующее сбою. При этом в АИС не должно происходить потери (либо потери должны быть минимальны) и искажения данных.
- 3.6. **Средства администрирования, управления и поддержки:**
- 3.7. В состав АИС должны быть интегрированы графические средства администрирования и/или утилиты командной строки, обеспечивающие эффективное полномасштабное и гибкое управление (в том числе мониторинг).

4. Среда безопасности АИС

- 4.1. Модели угроз, характерные для АИС
- 4.2. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся.
- 4.3. Источники угрозы – внешний злоумышленник.
- 4.4. Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств.
- 4.5. Используемые уязвимости – возможные недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления с передаваемой информацией третьих лиц.
- 4.6. Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.
- 4.7. Нарушаемое свойство безопасности – конфиденциальность.
- 4.8. Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации. Нанесение косвенного материального ущерба образовательному учреждению.
- 4.9. **Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся и их модификация (в том числе подмена).**
- 4.10. Источники угрозы – внешний злоумышленник.
- 4.11. Способ (метод) реализации угрозы – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств;

- модификация (в том числе подмена) перехваченной информации и навязывание ложной информации.
- 4.12. Используемые уязвимости – недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления и модификации (в том числе подмены) передаваемой информации.
- 4.13. Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.
- 4.14. Нарушаемые свойства безопасности – конфиденциальность, целостность.
- 4.15. Возможные последствия реализации угрозы – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации из-за несанкционированного раскрытия конфиденциальной информации или распространения раскрытых данных. Нанесение косвенного материального ущерба ДДТ.
- 4.16. **Нарушение доступности, утрата или искажение предоставляемых персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения.**
- 4.17. Источники угрозы – программное и аппаратное обеспечение.
- 4.18. Способ (метод) реализации угрозы – сбои (отказы) программного и аппаратного обеспечения.
- 4.19. Используемые уязвимости – недостатки механизмов обеспечения доступности требуемой информации, связанные с возможностью блокирования предоставления информации на недопустимое время.
- 4.20. Вид информации, потенциально подверженной угрозе – персональные данные работников и обучаемых.
- 4.21. Нарушаемое свойство безопасности – доступность, достоверность.
- 4.22. Возможные последствия реализации угрозы – нарушение со стороны образовательного учреждения взятых на себя обязательств по обработке персональных данных работников и обучающихся и может привести к прямому или косвенному материальному ущербу образовательному учреждению.
- 4.23. **Нарушение согласованности данных в персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения, а также ошибок персонала образовательного учреждения.**
- 4.24. Источники угрозы – программное и аппаратное обеспечение, персонал образовательного учреждения.
- 4.25. Способ (метод) реализации угрозы – сбои (отказы) программного обеспечения и ошибки персонала образовательного учреждения.
- 4.26. Используемые уязвимости – недостатки механизмов обеспечения согласованности данных в БД АИС, связанные с возможностью нарушения согласованности.
- 4.27. Вид информации, потенциально подверженной угрозе – персональные данные работников и обучающихся.
- 4.28. Нарушаемые свойства безопасности активов – достоверность, целостность.
- 4.29. Возможные последствия реализации угрозы – рассогласование в персональных данных работников и обучаемых, хранимых в БД АИС, что, в свою очередь, приведет к возможному нанесению морального и/или материального ущерба образовательному учреждению.
- 4.30. **Осуществление доступа (ознакомления) с персональными данными обучающегося, хранимыми и обрабатываемыми в АИС, без согласия субъекта персональных данных или окончания срока действия такого согласия.**
- 4.31. Источники угрозы – уполномоченные на доступ к персональным данным внутренние и внешние пользователи.

- 4.32. Способ (метод) реализации угрозы – осуществление доступа к персональным данным обучающихся с использованием штатных средств, предоставляемых программно-аппаратным обеспечением АИС.
- 4.33. Используемые уязвимости – недостатки механизмов защиты персональных данных обучающегося, связанные с возможностью доступа к ним без письменного согласия субъекта персональных данных или после окончания срока его действия.
- 4.34. Вид информации, потенциально подверженной угрозе – персональные данные обучающихся.
- 4.35. Нарушаемые свойства безопасности – конфиденциальность.
- 4.36. Возможные последствия реализации угрозы – несанкционированное ознакомление с персональными данными ведет к нанесению морального и/или материального ущерба обучающемуся из-за несанкционированного раскрытия конфиденциальной информации.
- 4.37. **Внедрение в информационную систему ДДТ вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами, а также пользователями с носителей информации, используемых на автоматизированных рабочих местах.**
- 4.38. Источники угрозы – внутренние пользователи и персонал ДДТ, внешние системы.
- 4.39. Способ (метод) реализации угрозы – внедрение вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами (файловый обмен, электронная почта и т.п.), а также при использовании съемных носителей информации на автоматизированных рабочих местах.
- 4.40. Используемые уязвимости – недостатки механизмов защиты информационной системы образовательного учреждения от внедрения вирусов и другого вредоносного программного обеспечения, связанные с возможностью внедрения вирусов и другого вредоносного программного обеспечения.
- 4.41. Вид информации, потенциально подверженной угрозе – программное обеспечение информационной системы ДДТ.
- 4.42. Нарушаемое свойство безопасности активов – целостность.
- 4.43. Возможные последствия реализации угрозы – нарушение режимов функционирования информационной системы ДДТ, потеря (утрата) и искажение информации, снижение уровня защищенности информационной системы ДДТ. Ведет к возможному материальному ущербу ДДТ.
- 4.44. **Осуществление несанкционированных информационных воздействий (модификация конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.) на информационную систему ДДТ, осуществляемых из внешних систем.**
- 4.45. Источники угрозы – внешние злоумышленники, внешние системы.
- 4.46. Способ (метод) реализации угрозы – несанкционированные информационные воздействия с использованием специализированного программно-аппаратного обеспечения.
- 4.47. Используемые уязвимости – недостатки механизмов защиты информационной системы образовательного учреждения от несанкционированных внешних воздействий.
- 4.48. Вид информации, потенциально подверженной угрозе – программно-аппаратное обеспечение информационной системы ДДТ.
- 4.49. Нарушаемые свойства безопасности активов – конфиденциальность, целостность.
- 4.50. Возможные последствия реализации угрозы – нарушение режимов функционирования информационной системы ДДТ, снижение уровня защищенности информационной системы ДДТ. Ведет к возможному материальному ущербу ДДТ.
- 4.51. **Политика и цели безопасности для АИС.**
- 4.52. АИС должна обеспечить следование приведенным ниже правилам безопасности:

- 4.53. Должна быть обеспечена регистрация и учет получения (включая указание срока действия) согласия обучающегося (законных представителей) на обработку предоставленных им в ДДТ своих персональных данных.
- 4.54. Должна быть обеспечена возможность надежного хранения персональных данных работников и обучающихся (в течение действия срока трудового договора и разрешения на обработку персональных данных соответственно).
- 4.55. Должна быть обеспечена возможность безопасного восстановления АИС после сбоев и отказов программного обеспечения и оборудования.
- 4.56. Должна быть обеспечена защита информации, составляющей персональные данные работников и обучающихся, при ее обработке, хранении и передаче специализированными средствами защиты.
- 4.57. Должно быть обеспечено наличие надлежащих, защищенных от несанкционированного использования, механизмов регистрации и предупреждения администратора АИС о любых событиях, относящихся к безопасности АИС.
- 4.58. Должно быть обеспечено наличие надлежащих и корректно функционирующих средств администрирования безопасности информационной системы ДДТ, доступных только уполномоченным администраторам.
- 4.59. Должны быть предоставлены механизмы аутентификации, обеспечивающие адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с низким потенциалом нападения.
- 4.60. Должны быть обеспечены механизмы генерации, надлежащего и защищенного распределения, уничтожения ключевой информации, а также механизмы шифрования, и формирования электронной цифровой подписи. Данные механизмы должны функционировать в соответствии с сертифицированными алгоритмами.
- 4.61. **Политика и цели безопасности для среды функционирования АИС.**
- 4.62. Среда функционирования АИС должна обеспечить следование приведенным ниже правилам безопасности:
- Должна быть обеспечена инженерно-техническая укрепленность объектов размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных.
 - Объекты размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должны быть оборудованы системой охранной сигнализации.
 - Должна быть исключена возможность несанкционированного физического доступа к программно-аппаратным элементам системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, со стороны посторонних лиц.
 - На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено наличие и надлежащее использование средств антивирусной защиты, сертифицированных по требованиям безопасности. Должно быть обеспечено регулярное обновление антивирусных баз.
 - Объекты системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть подключены к внешним вычислительным сетям общего пользования с использованием надлежащих средств межсетевого экранирования, сертифицированных по требованиям безопасности.
 - На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено отсутствие нештатных программных средств, не имеющих отношение к процессу функционирования ДДТ.
 - Должны быть обеспечены установка, конфигурирование и управление программно-аппаратными средствами АИС в соответствии с руководствами и согласно оцененным конфигурациям.

- Персонал, ответственный за администрирование АИС, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.
- Уполномоченные на работу с АИС операторы должны быть благонадежными, руководствоваться в своей работе эксплуатационной документацией на АИС, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.