МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ЦЕНТР ДЕТСКО-ЮНОШЕСКОГО ТВОРЧЕСТВА»

ПРИНЯТО
на общем собрании работников
МБУ ДО «ЦДЮТ»
Протокол № 2 от 01 октября 2021 г.

УТВЕРЖДАЮ
Директор МБУ ДО «ЦДЮТ»
_____Т.Р. Садыков
Введено в действие приказом
№ 168 от 01 октября 2021 г.

ПОЛИТИКА
информационной безопасности
МБУ ДО «Центр детско-юношеского творчества»

1. Общие положения

1. Понятия и термины, применяемые в настоящей политике, используются в значениях, установленных:

- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 09.03.2021г.);
- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Законодательной основой политики являются Конституция Российской Федерации, Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации.

3. Политика предназначена для обеспечения общих основ информационной безопасности и выбора практических мероприятий по обеспечению и управлению информационной безопасностью в МБУ ДО «Центр детско-юношеского творчества» (далее - ЦДЮТ).

4. ЦДЮТ обязан соблюдать требования настоящей политики и законодательства Российской Федерации в сфере информационной безопасности.

5. Работники ЦДЮТ, ответственные за информационную безопасность, разрабатывают на местах организационно-распорядительную документацию, дополняющую данную политику.

2. Объекты защиты

6. Объектами защиты МБУ ДО «ЦДЮТ» являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

3. Цели и задачи обеспечения информационной безопасности

7. Целью информационной безопасности является обеспечение непрерывности работы МБУ ДО «ЦДЮТ» при выполнении своих полномочий и функций.

8. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих основных свойств объектов защиты:

- конфиденциальность;
- целостность;
- доступность.

9. Необходимый уровень конфиденциальности, целостности и доступности обеспечивается соответствующими множеству значимых факторов, воздействующих на безопасность информации, мерами и средствами обеспечения информационной безопасности.

10. Задачами для достижения цели информационной безопасности являются:

- организация системы менеджмента информационной безопасности;
- своевременное выявление, оценка и прогнозирование факторов, воздействующих на безопасность информации, причин и условий, способствующих нарушению нормального функционирования информационных систем органов власти и учреждений;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;
- защита от несанкционированного доступа к объектам защиты;
- защита от несанкционированной модификации используемых в информационных системах органов власти и учреждений программных средств, а также защита информационных систем от внедрения несанкционированных программ, включая компьютерные вирусы;
- определение основных принципов информационной безопасности;
- определение мер и средств обеспечения информационной безопасности.

11. Поставленные цели и решение задач достигаются:

- строгим учетом всех объектов защиты;
- категорированием и классификацией информационных систем и ресурсов для обеспечения защиты на надлежащем уровне;
- регистрированием действий работников МБУ ДО «ЦДЮТ», осуществляющих обслуживание объектов защиты;
- распределением обязанностей по обеспечению информационной безопасности. Полномочия работников должны быть четко определены и закреплены должностными регламентами (инструкциями), в том числе в служебных контрактах (трудовых договорах) с работниками Управления образования и учреждений;
- выполнением всеми пользователями информационных систем МБУ ДО «ЦДЮТ» требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- персональной ответственностью за свои действия каждого работника, имеющего доступ к объектам защиты органов власти и учреждений, в рамках своих функциональных обязанностей;
- повышением квалификации работников, ответственных за защиту информации в МБУ ДО «Центр детско-юношеского творчества»;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов МБУ ДО «ЦДЮТ» по вопросам обеспечения информационной безопасности;
- систематической оценкой рисков. Решения о расходах на мероприятия по информационной безопасности в МБУ ДО «ЦДЮТ» должны приниматься исходя из возможного ущерба в результате нарушения информационной безопасности;
- непрерывным поддержанием необходимого уровня информационной безопасности МБУ ДО «Центр детско-юношеского творчества»;
- применением физических и технических (программно-аппаратных) средств защиты информационных ресурсов МБУ ДО «ЦДЮТ»;
- эффективным контролем над соблюдением пользователями информационных ресурсов требований по обеспечению информационной безопасности.

4. Система менеджмента информационной безопасности

12. Система менеджмента информационной безопасности предназначена для создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы защиты информации в МБУ ДО «ЦДЮТ» при выполнении своих функций.

13. Основные принципы системы менеджмента информационной безопасности:

- понимание необходимости системы информационной безопасности;
- назначение ответственности за информационную безопасность;
- создание административных обязанностей работников МБУ ДО «ЦДЮТ», ответственных за обеспечение информационной безопасности;
- оценка риска, определяющая соответствующие меры и средства контроля и управления информационной безопасностью;
- обеспечение комплексного подхода к менеджменту информационной безопасности;
- выявление и предупреждение инцидентов информационной безопасности;
- непрерывная переоценка и соответствующая модификация системы информационной безопасности.

14. Для непосредственной организации и эффективного функционирования системы менеджмента информационной безопасности, исключающей возможные конфликты интересов, в МБУ ДО «Центр детско-юношеского творчества» целесообразно создать подразделение (назначить лицо), ответственное за обеспечение информационной безопасности, и возложить на него решение следующих основных задач:

- реализация политики информационной безопасности, определение требований к системе защиты информации;
- анализ текущего состояния обеспечения информационной безопасности;
- организация мероприятий и координация работ по защите информации МБУ ДО «Центр детско-юношеского творчества»;
- контроль и оценка эффективности применяемых мер и средств защиты информации.

15. Основными функциями подразделений (лиц), ответственных за обеспечение информационной безопасности МБУ ДО «ЦДЮТ», являются:

- формирование требований к системам защиты в процессе создания и дальнейшего развития существующих объектов защиты;
- подготовка решений по обеспечению конфиденциальности, целостности, доступности объектов защиты;
- участие в проектировании систем защиты, их испытаниях и приемке в эксплуатацию;
- обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;
- разграничение доступа пользователей к объектам защиты;
- наблюдение за функционированием системы защиты и ее элементов;
- проверка надежности функционирования системы защиты;

- разработка мер нейтрализации моделей возможных атак;
- обучение работников правилам безопасной обработки информации;
- контроль соответствия действий администраторов и пользователей установленным правилам обращения с информацией;
- участие по указанию руководства в служебной проверке по фактам нарушения правил обращения с информацией и оборудованием в учреждениях в соответствии с законодательством Российской Федерации;
- сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности.

5. Факторы, воздействующие на безопасность информации

16. Выявление и учет факторов, воздействующих на защищаемую информацию, составляют основу для планирования и проведения эффективных мероприятий по информационной безопасности.

17. Выявление факторов, воздействующих на безопасность информации, должно осуществляться с учетом следующих требований:

- достаточности уровней классификации факторов, позволяющих формировать их полное множество;
- гибкость классификации, позволяющей расширять множества классифицируемых факторов, а также вносить необходимые изменения без нарушения структуры классификации.

18. Все множество факторов, воздействующих на защищаемую информацию, по природе их возникновения разделяются на два класса:

- Объективные – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;
- Субъективные – это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить непреднамеренные и преднамеренные. Непреднамеренные угрозы вызваны ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п. Преднамеренные угрозы связанны с корыстными, идейными или иными устремлениями людей (злоумышленников).

19. По отношению к объектам защиты факторы разделяются на внутренние и внешние.

20. Основными факторами, воздействующими на безопасность информации, для МБУ ДО «Центр детско-юношеского творчества» являются:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационных систем органов власти и учреждений (в том числе работников, отвечающих за обслуживание и администрирование информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению, потере конфиденциальной информации или нарушению работоспособности информационных систем МБУ ДО «ЦДЮТ»;

- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом, халатность и т.п.) действия легально допущенных к информационным ресурсам МБУ ДО «ЦДЮТ» пользователей (в том числе работников, отвечающих за обслуживание и администрирование информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению, потере конфиденциальной информации или нарушению работоспособности информационных систем органов власти и учреждений;
- деятельность преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности информационных систем МБУ ДО «Центр детско-юношеского творчества»;
- ошибки, допущенные при разработке компонентов информационных систем МБУ ДО «ЦДЮТ» и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты);
- явления техногенного характера, стихийные бедствия.

21. Реализация основных объективных факторов, воздействующих на безопасность информации, возможна путем:

- выхода из строя оборудования и программных средств информационных систем МБУ ДО «Центр детско-юношеского творчества»;
- выхода из строя или невозможность использования линий связи;
- пожаров, наводнений и других стихийных бедствий, и явлений техногенного характера.

22. Реализация непреднамеренных субъективных факторов, воздействующих на безопасность информации, возможна путем:

- неумышленных действий, приводящих к частичному или полному нарушению функциональности компонентов информационных систем органов власти и учреждений или разрушению информационных, или программно-технических ресурсов;
- неосторожных действий, приводящих к разглашению информации ограниченного распространения или делающих ее общедоступной;
- разглашения, передачи или утраты атрибутов разграничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т. п.);
- игнорирования организационных правил при работе с информационными ресурсами;
- проектирования архитектуры систем, технологий обработки данных, разработки программного обеспечения с возможностями, представляющими опасность для функционирования информационных систем МБУ ДО «ЦДЮТ» и информационной безопасности;
- пересылки данных и документов по ошибочному адресу (устройства);
- ввода ошибочных данных;
- неумышленной порчи и утраты носителей информации;
- неумышленного повреждения каналов связи;

- неправомерного отключения оборудования или изменения режимов работы устройств или программ;
- заражения компьютеров вирусами;
- несанкционированного запуска технологических программ, способных вызвать потерю работоспособности информационных систем МБУ ДО «ЦДЮТ» или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- некомпетентного использования, настройки или неправомерного отключения средств защиты.

23. Реализация преднамеренных субъективных факторов, воздействующих на безопасность информации, возможна путем:

- умышленных действий, приводящих к частичному или полному нарушению функциональности информационных систем МБУ ДО «Центр детско-юношеского творчества» или разрушению информационных или программно-технических ресурсов;
- действий по дезорганизации функционирования информационных систем органов власти и учреждений;
- хищения документов и носителей информации;
- несанкционированного копирования документов и носителей информации;
- умышленного искажения информации, ввода неверных данных;
- отключения или вывода из строя подсистем обеспечения функционирования информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);
- перехвата данных, передаваемых по каналам связи, и их анализа;
- хищения производственных отходов (распечаток документов, записей, носителей информации и т.п.);
- незаконного получения атрибутов разграничения доступа (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);
- несанкционированного доступа к ресурсам информационных систем МБУ ДО «Центр детско-юношеского творчества» с рабочих станций легальных пользователей;
- хищения или вскрытия шифров криптозащиты информации;
- внедрения аппаратных и программных закладок с целью скрытного осуществления доступа к информационным ресурсам или дезорганизации функционирования информационных систем МБУ ДО «ЦДЮТ»;
- незаконного использования оборудования, программных средств или информационных ресурсов, нарушающие права третьих лиц;
- применения подслушивающих устройств, дистанционной фото - и видео съемки для несанкционированного съема информации.

6. Основные принципы информационной безопасности

24. При построении системы информационной безопасности МБУ ДО «Центр детско-юношеского творчества» необходимо руководствоваться следующими основными принципами:

- законность (осуществление защитных мероприятий и разработки системы информационной безопасности МБУ ДО «ЦДЮТ» в соответствии с действующим законодательством в области защиты информации);
- системность (учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности);
- комплексность (согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов);
- непрерывность (постоянная работа и организационная поддержка мер и средств защиты для эффективного обеспечения информационной безопасности);
- своевременность (постановка задач по комплексной защите информации и реализация мер обеспечения информационной безопасности на ранних стадиях разработки информационных систем в целом и их систем защиты информации в частности);
- преемственность и непрерывность совершенствования (совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и систем их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите);
- разумная достаточность (выбор достаточного уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми);
- персональная ответственность (ответственность за обеспечение информационной безопасности для каждого работника МБУ ДО «ЦДЮТ» в пределах его полномочий);
- минимизация полномочий (предоставление пользователям минимальных прав в соответствии с должностными регламентами, должностными инструкциями работников МБУ ДО «Центр детско-юношеского творчества»);
- исключение конфликта интересов (четкое разделение обязанностей работников МБУ ДО «Центр детско-юношеского творчества» и исключение ситуаций, когда сфера ответственности допускает конфликт интересов);
- взаимодействие и сотрудничество (работники МБУ ДО «Центр детско-юношеского творчества» должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений (ответственных лиц) за обеспечение информационной безопасности);
- гибкость системы защиты (способность реагировать на изменения внешней среды и условий осуществления МБУ ДО «ЦДЮТ» своих функций);
- простота применения средств защиты (не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при работе

пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций);

- обоснованность и техническая реализуемость (реализация на современном уровне развития науки и техники, обоснованность с точки зрения достижения заданного уровня безопасности информации, а также соответствие установленным нормам и требованиям по безопасности информации);
- специализация и профессионализм (реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными работниками);
- обязательность контроля (обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств).

7. Меры и средства обеспечения информационной безопасности

25. При осуществлении менеджмента информационной безопасности необходимо выделить следующие основные меры обеспечения информационной безопасности:

- законодательные (законодательство Российской Федерации в сфере информационной безопасности). Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с работниками МБУ ДО «Центр детско-юношеского творчества»;
- морально-этические (нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе). Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в МБУ ДО «Центр детско-юношеского творчества»;
- технологические (технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий);
- организационные (меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность работников, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации);
- физические (меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для предотвращения несанкционированного доступа к объектам защиты, а также технических средств визуального наблюдения, связи и охранной сигнализации);

- технические (меры защиты основаны на использовании различных электронных устройств и специального программного обеспечения, выполняющего функции защиты).

26. Для обеспечения информационной безопасности необходимо использовать средства:

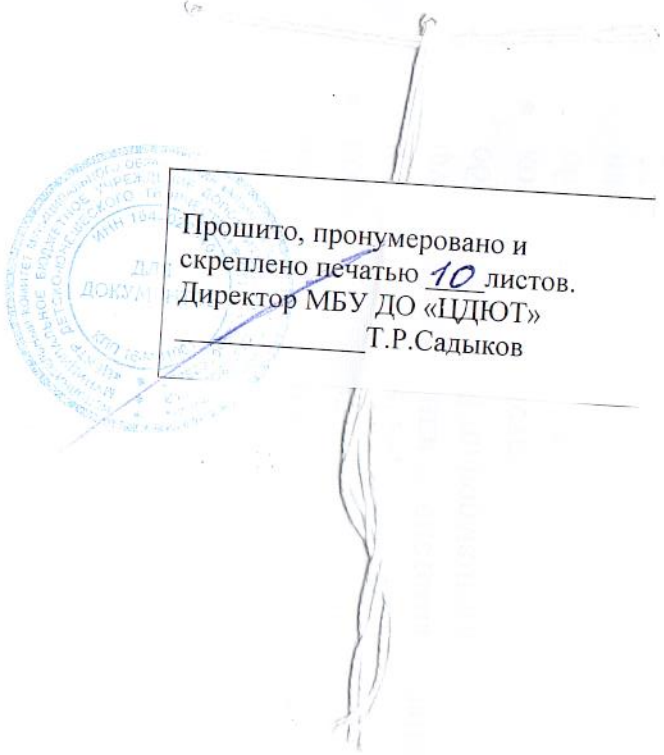
- физической защиты (введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки конфиденциальной информации, оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи);
- антивирусной защиты (предотвращение потерь, ошибок и модификации информационных ресурсов);
- резервирования (поддержание целостности и доступности объектов защиты);
- разграничения доступа (управление доступом к информационным ресурсам, к сети общего пользования, к локальной вычислительной сети);
- криптографической защиты (защита конфиденциальности, целостности и аутентичности информационных ресурсов путем применения средств криптографической защиты информации, в том числе при передаче по каналам связи);
- идентификации и аутентификации (предотвращение работы с информационными ресурсами посторонних лиц путем обеспечения возможности распознавания каждого легального пользователя);
- контроля целостности (своевременное обнаружение модификации или искажения информационных ресурсов, обеспечение правильности функционирования системы защиты и целостности хранимой и обрабатываемой информации);
- контроля и регистрации событий информационной безопасности (обеспечение обнаружения и регистрации всех событий, которые могут повлечь за собой нарушение информационной безопасности).

27. При выполнении договорных отношений между МБУ ДО «Центр детско-юношеского творчества» и сторонними организациями (предоставление доступа сторонним организациям к объектам защиты) обязательно выполнение всех необходимых мер и средств обеспечения информационной безопасности.

28. В служебной деятельности работники МБУ ДО «Центр детско-юношеского творчества» обязаны использовать адреса электронной почты, зарегистрированные в почтовом домене tatar.ru, запрещается использование сторонних серверов и сервисов электронной почты.

8. Ответственность за нарушение обеспечения информационной безопасности

29. Нарушение информационной безопасности может повлечь дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.



Прошито, пронумеровано и
скреплено печатью 10 листов.
Директор МБУ ДО «ЦДЮТ»
_____Т.Р.Садыков