

Утверждаю
Директор МБУ ДО ЦТ «Созвездие»
МО Усть-Лабинский район


Н.И. Журавская
« 09 » сентября 2023 г.

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МБУ ДО ЦТ «СОЗВЕЗДИЕ» МО Усть-Лабинский район

1. Назначение и правовая основа политики информационной безопасности

1.1. Настоящее Положение об информационной безопасности Муниципального бюджетного учреждения дополнительного образования Центр творчества «Созвездие» (далее – Учреждение) определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих Положений, Правил, Инструкций.

1.2. Настоящее Положение является документом, доступным любому сотруднику Учреждения и пользователю его ресурсов, и представляет собой официально принятую руководством Учреждения систему взглядов на проблему обеспечения информационной безопасности.

1.3. Руководство Учреждения осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства, а также ожиданий педагогического и рабочего состава Учреждения, обучающихся и их родителей и других заинтересованных сторон. Обеспечение информационной безопасности – необходимое условие для успешного осуществления образовательной деятельности Учреждения. Нарушения в данной области могут привести к серьезным последствиям, включая потерю доверия со стороны преподавательского и рабочего состава Учреждения, обучающихся и их родителей.

1.4. Настоящее Положение разработано в соответствии с законодательством Российской Федерации и нормами права в части обеспечения безопасности защищаемой информации, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим средствам разведки и технической защиты информации, и основывается, в том числе, на:

- Доктрине информационной безопасности Российской Федерации (Утверждена Указом Президента Российской Федерации от 01.05.2022 года № 250).

- Федеральном законе от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральном законе от 14.07.2022 года № 266-ФЗ «О внесении изменений в Федеральный закон о персональных данных».
- Федеральном законе от 06.04.2011 года № 63-ФЗ «Об электронной подписи».
- Федеральном законе от 29.12.2012 года № 273-ФЗ «Об образовании в Российской Федерации».
- Распоряжении Правительства РФ от 01.12.2015 года № 2471-р «Об утверждении Концепции информационной безопасности детей».

1.2. Необходимые требования обеспечения информационной безопасности Учреждения должны неукоснительно соблюдаться сотрудниками и рабочим персоналом Учреждения и другими сторонами как это определяется положениями внутренних нормативных документов Учреждения, а также требованиями договоров и соглашений, стороной которых является Учреждение.

1.3. Настоящая Положение предназначено для сотрудников Учреждения выполнение должностных обязанностей которых связано с использованием персональных компьютеров.

2. Термины и определения

В настоящей Положении использованы термины с соответствующими определениями законодательства Российской Федерации и норм права в части обеспечения информационной безопасности, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

2.1. **Информация** - сведения (сообщения, данные) независимо от формы их представления.

2.2. **Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

2.3. **Информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

2.4. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.5. **Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.6. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными,

включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.7. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

2.8. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.9. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.10. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.11. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.12. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.13. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

2.14. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.15. Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.16. Режим обработки персональных данных - организационно-технические мероприятия по защите персональных данных, позволяющие Оператору персональных данных при существующих или возможных обстоятельствах обеспечить целостность, доступность и конфиденциальность персональных данных, избежать неоправданных расходов, и реализующие меры по охране персональных данных, включающие в себя:

- определение перечня персональных данных в соответствии с целями и задачами обработки, требованиями Федерального закона от 27.07.2006 года №152 «О персональных данных»;
- ограничение доступа к персональным данным путем установления порядка обращения с ними и контроля за соблюдением такого порядка;
- определение класса информационной системы, в которой осуществляется обработка персональных данных;
- учет лиц, получивших доступ к персональным данным, и (или) лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию персональных данных работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров и соглашений.

2.17. Рисковое событие информационной безопасности - это событие, обусловленное операционным риском, повлекшее или способное повлечь за собой потери Учреждения и произошедшее по причине ошибочности или сбоя процессов Учреждения, действий людей и систем, а также по причине внешних событий.

2.18. Угроза информационной безопасности - операционный риск, влияющий на нарушение одного (или нескольких) свойств информации - целостности, конфиденциальности, доступности.

2.19. Уязвимость – любая характеристика автоматизированной системы, использование которой может привести к реализации угроз.

3. ЦЕЛИ И ЗАДАЧИ, ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1 Целями деятельности по обеспечению информационной безопасности Учреждения являются:

- снижение угроз информационной безопасности до приемлемого для Учреждения уровня;
- защита персональных данных, обрабатываемых в информационной системе Учреждения; защита информационной системы от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи;
- минимизация уровня рисков;
- определение степени ответственности и обязанностей сотрудников по обеспечению. Информационной безопасности.

3.1 Основные задачи деятельности по обеспечению информационной безопасности Учреждения:

- отнесение информации к категории несекретной, ограниченного распространения, коммерческой и другим видам тайн, иной конфиденциальной информации, информации персонального характера подлежащей защите от неправомерного использования;
- прогнозирование и своевременное выявление угроз безопасности информационным ресурсам Учреждения, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- создание условий функционирования Учреждения с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и нанесения ущерба;
- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании Учреждения, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного предотвращения и

локализации ущерба, наносимого неправомерными действиями физических и (или) юридических лиц;

- защита информации Учреждения от несанкционированного доступа (далее – НСД) и утечки по техническим каналам связи.

3.2 Построение системы обеспечения безопасности информации Учреждения и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- **законности** – соблюдение законодательства по защите информации, защите персональных данных и законных интересов всех участников информационного обмена;

- **системности** – подход к вопросам организации информационной безопасности должен быть логическим и последовательным: в первую очередь категорирование обрабатываемой информации, информационной системы, оценка риска информационной безопасности исходя из реальных угроз и уязвимости информационных ресурсов, затем создание комплекса организационных и технических мер и средств защиты, учитывающих специфику Учреждения;

- **эффективности** – реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению информационной безопасности должны сводить риски к приемлемому уровню, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе;

- **целесообразности** – соблюдение соразмерности затрат на обеспечение защиты информации и потенциальных потерь при реализации угроз;

- **непрерывности** – принцип функционирования системы информационной безопасности, учитывающий, что злоумышленники в любой момент времени ищут возможность обхода защитных мер, прибегая для этого к легальным и нелегальным методам;

- **взаимодействии и координации** – осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи структурных подразделений Учреждения, информационных технологий и подразделений-пользователей информационных ресурсов, сторонних специализированных организаций в области защиты информации и обслуживания информационных систем, координации их усилий для достижения поставленных целей, а также взаимодействия с уполномоченными государственными органами. Эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться подготовленными сотрудниками Учреждения;

- **совершенствовании** – совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;

- **приоритетности** – категорирование (ранжирование) информации и всех информационных ресурсов Учреждения по степени важности и оценка реальных, а также потенциальных угроз информационной безопасности;

- **информированности и персональной ответственности** – пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации, информационных сервисов индивидуально

– идентифицирующих и аутентифицирующих пользователей и

инициируемые ими процессы;

▪ **обязательность контроля** – контроль за деятельностью пользователей, а также мониторинг работы информационной системы должен осуществляться на основе применения средств оперативного контроля и регистрации, охватывать как несанкционированные, так и санкционированные действия.

4. ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1 Требования об обеспечении информационной безопасности Учреждения и обработке персональных данных обязательны к соблюдению всеми работниками Учреждения и пользователями информационных систем.

4.2 Руководство Учреждения приветствует и поощряет в установленном порядке деятельность работников Учреждения и пользователей информационных систем по обеспечению информационной безопасности.

4.3 Неисполнение или некачественное исполнение сотрудниками Учреждения и пользователей информационных систем обязанностей по обеспечению информационной безопасности и обработке персональных данных может повлечь применение к виновным административных мер воздействия, степень которых определяется установленным в Учреждении порядком либо требованиями действующего законодательства.

4.4 Все работы в пределах Учреждения должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.

4.5 В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

4.6 Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись, в том числе членам своей семьи и близким.

4.7 Доступ в сеть «Интернет» предоставляется сотрудникам исключительно для выполнения ими своих функциональных обязанностей.

4.8 Для работы в сети «Интернет» используются автоматизированные рабочие места, удовлетворяющие техническим требованиям, необходимым для выполнения этих задач. В качестве программного обеспечения для работы в сети «Интернет», рекомендуются к использованию. Яндекс Браузер. Возможно использование других браузеров либо лицензионных, либо свободно распространяемых, при согласовании с ответственным за информационную безопасность.

4.9 Рекомендательные правила:

- сотрудникам Учреждения разрешается использовать сеть «Интернет» только в служебных целях;

- работа сотрудников Учреждения с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Учреждения в сеть «Интернет»;

4.10 При работе в сети «Интернет» сотрудникам запрещается:

- загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;

- использование информационных ресурсов в личных целях;

- запрещается посещение любого сайта Интернет, который считается оскорбительным для общественного мнения или содержит информацию пропаганды расовой ненависти, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу религиозных или политических убеждений, национального происхождения или недееспособности;

- несанкционированное распространение информации рекламного характера;
- запрещен доступ в «Интернет» через сеть Учреждения для всех лиц. Не являющихся сотрудниками Учреждения, включая членов семьи сотрудников;

4.11 Все компьютерное (стационарные компьютеры и ноутбуки), периферийное оборудование (принтеры), аксессуары (манипуляторы типа «мыши», дисководы для СД-дисков) является собственностью Учреждения и предназначено для использования исключительно в производственных целях.

4.12 Каждый сотрудник, получивший в пользование ноутбук или компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

4.13 Все компьютеры и ноутбуки должны защищаться паролем при загрузке системы, активации горячей клавиши и после выхода из режима «Экранной заставки». Перед утилизацией все компоненты оборудования, в состав которых входят носители данных необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных.

4.14 Сотрудники Учреждения для обмена документами должны использовать только свой официальный адрес электронной почты.

4.15 Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности.

4.16 Ответственность за сохранность данных на стационарных компьютерах и ноутбуках лежит на пользователе.

Технические меры обеспечения информационной безопасности включают в себя:

- обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам информационных систем Учреждения и информации, обрабатываемой в них;

- применение программных, программно-аппаратных средств криптографической защиты информации;

- обеспечение бесперебойной работы информационной системы обработки персональных данных и сети связи;

- обеспечение возобновления работы информационных ресурсов и сети связи после прерываний и нештатных ситуаций;

- применение средств защиты от вредоносных программ;

- применение средств обнаружения вторжений;

- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;

- предотвращения несанкционированного изменений программ и оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.;

- проверку машинных и ручных протоколов выполнения работ со стороны пользователей;

- применение мер и технических средств, снижающих вероятность

несанкционированного получения информации в устной форме (пассивная защита);

4.17 Управление инцидентами информационной безопасности в Учреждении включает в себя:

- сбор информации о событиях информационной безопасности;
- выявление и анализ инцидентов информационной безопасности;
- расследование инцидентов информационной безопасности;
- оперативное реагирование на инцидент информационной безопасности;
- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства Учреждения информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
- выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности.

4.18 За одним рабочим местом должно находиться не более одного сотрудника. Запрещается работать под чужим регистрационным именем, сообщать кому-либо свой пароль, входить в систему более чем с одного персонального устройства, допускать к оборудованию посторонних лиц.

4.19 Сотруднику разрешается записывать полученную служебную информацию из сети «Интернет» на личные носители информации, предварительно проверенные на наличие вирусов. Запрещено копировать на личные носители информацию с персональными данными и информацию ограниченного использования.

4.20 Сотрудник обязан помнить свой пароль.

4.21 Не позже, чем за две недели до увольнения сотрудник обязан передать все доступы и пароли, полученные, либо созданные и используемые им для выполнения своих функциональных обязанностей.

4.22 При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния, удаление информации на Интернет-ресурсах, информационных материалов) сотрудник несет ответственность в соответствии с действующим законодательством РФ.

4.23 Доступ к информационным системам сети «Интернет» для обучающихся отсутствует.

5. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1 Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

- несанкционированное распространение (передача) персональных данных;
- утрата сведений, составляющих конфиденциальную информацию, персональные данные Учреждения и иную защищаемую информацию, а также

искажение такой информации;

- утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.);

- недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, систем управления баз данных, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;

- отсутствие планирования и контроля;
- низкая степень надежности программного обеспечения;
- недостаточная осведомленность персонала, низкая квалификация персонала и пользователей в области информационных технологий.

5.2 В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности Учреждения и его нормальное функционирование:

- финансовые потери, связанные с утечкой или разглашением защищаемой информации;

- финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;

- ущерб от дезорганизации деятельности Учреждения и потери, связанные с невозможностью выполнения им своих обязательств;

- моральные потери (ущерб репутации Учреждения).

6. СПОСОБЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

6.1 Человеческий. Информация может быть похищена путем копирования на временные носители, направлена по электронной почте. При наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

6.2. Программный. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, внесение изменений в работу иных программ.

6.3. Аппаратный. Способ связан или с использованием специальных технических средств или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

7. СТРУКТУРА УПРАВЛЕНИЯ ПОЛИТИКОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1 В целях выполнения задач по обеспечению информационной безопасности Учреждения, в Учреждении определены следующие роли:

- Руководитель Учреждения.
- Ответственный за обработку персональных данных.
- Педагоги дополнительного образования.
- Работники Учреждения.

7.2 При необходимости могут быть определены и другие роли по информационной безопасности.

7.3 Общее руководство обеспечением информационной безопасности Учреждения осуществляет руководитель Учреждения.

7.4 Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Учреждения лежит на **ответственном за обработку персональных данных**.

7.5 Ответственность педагогического состава и работников Учреждения за невыполнение настоящей Политики определяется законодательством Российской Федерации, а также положениями внутренних нормативных документов (локальных актов) Учреждения.

7.6 Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Учреждения осуществляются и координируются **ответственным за обработку персональных данных**.

7.7 Задачи ответственного за обработку персональных данных и педагогического состава Учреждения по обеспечению информационной безопасности определяются законодательством Российской Федерации и локальными актами **Учреждения**.

7.8 **Руководитель Учреждения** может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые ответственным за обработку персональных данных, и может, при необходимости привлекать для работы в них ответственных сотрудников Учреждения на основе совмещения работы в группе со своими основными должностными обязанностями.

7.9 Финансирование работ по реализации положений настоящей Политики осуществляется в рамках бюджета Учреждения.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1 Положение ступает в силу с момента его утверждения.

8.2 Положение является локальным актом. Внесение изменений и дополнений в Положение осуществляется в порядке его принятия.

8.3 В случае изменения действующего законодательства и иных нормативных актов, а также Устава Учреждения настоящее Положение и изменения к нему применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Учреждения. В этом случае ответственный за обработку персональных данных обязан незамедлительно инициировать внесение соответствующих изменений.

8.4 Внесение изменений в настоящее Положение осуществляется на периодической и внеплановой основе:

- периодическое внесение изменений в настоящее Положение должно осуществляться не реже одного раза в 12 месяцев;

- внеплановое внесение изменений в настоящее Положение может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.