Управление образования Администрации Людиновского
муниципального округа Калужской области
Муниципальное казенное образовательное учреждение
дополнительного образования «Дом детского творчества»

СОГЛАСОВАНО
Председатель первичной профсоюзной
организации МКОУ ДО
«Дом детского творчества»
_____Т.В.Светлова
Протокол № ____
от «__» января 2026г

УТВЕРЖДАЮ
Директор МКОУ ДО
«Дом детского творчества»
Прохорова Татьяна Александровна
Подписано цифровой подписью: Прохорова Татьяна Александровна
Т.А. Прохорова
«___» ____01_____ 2026 г.

Политика
парольной защиты информационных систем

г. Людиново, 2026г.

Политика парольной защиты информационных систем

Настоящая политика парольной защиты информационных систем (далее – Политика) устанавливает порядок и правила генерации, использования паролей в информационных системах Учреждения, обязанности ответственного лица в области защиты информации в муниципальном казенном образовательном учреждении дополнительного образования «Дом детского творчества» (далее – Учреждении).

Бесконтрольность в определении и использовании паролей может повлечь риск несанкционированного доступа к информации Учреждения, повлечь мошеннические и другие действия в информационных системах, которые могут нанести материальный вред и ущерб репутации Учреждения.

Термины и определения

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности.

Аутентичность - свойство, гарантирующее, что субъект или ресурс идентичны с заявленным.

Безопасность информации - состояние защищенности информации, при котором обеспечены конфиденциальность, доступность и целостность.

Информационная безопасность - все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Доступность - свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационная технология - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Конфиденциальность - свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

Несанкционированный доступ - доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа.

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации

Персональные данные - любая информация, относящаяся к определенному физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, другая информация.

Ресурс системы обработки информации - средство системы обработки информации, которое может быть выделено процессу обработки данных на определенный интервал времени.

Средство обнаружения вторжений - средство обнаружения атак: Программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности.

Средство защиты от несанкционированного доступа - программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Средство защиты информации - техническое, программное средство, предназначенные или используемые для защиты информации.

Перечень используемых сокращений:

АРМ – автоматизированное рабочее место;

АС – автоматизированная система;

ИС – информационная система;

НСД – несанкционированный доступ;

ПДн – персональные данные;

РМ – рабочее место;

СрЗИ – средство защиты информации.

Общие положения

Настоящая Политика разработана в целях определения порядка парольной защиты ИС РМ работников в Учреждении.

Положения данной Политики должны учитываться при определении правил генерирования, использования, хранения, смены, прекращения действия паролей доступа к ИС, РМ работников, а также конкретным защищаемым информационным ресурсам, таким как приложения, хранилища информации, базы данных и т. п., входящим в состав указанных систем (далее – паролей).

В данной Политике не рассматриваются вопросы парольной защиты ИС и РМ, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну, а также ресурсов, содержащих такие сведения.

При разработке Политики учитывались требования следующих нормативно-методических документов РФ в области защиты информации:

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (с изменениями на 24 июня 2025 года) ;
2. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»(с изменениями на 24 июня 2025 года, редакция, действующая с 1 января 2026 года);
3. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»
4. Другими нормативно-правовыми актами и государственными стандартами.

Требования к парольной защите каждой отдельной ИС должны учитывать особенности технологического процесса обработки информации в системе, тип системы, а также максимальный уровень конфиденциальности обрабатываемой в ней информации.

Первоначальная учётная запись администратора изначально создаётся при установке домена, после чего учётная запись блокируется.

Пароли доступа к защищаемым информационным ресурсам должны генерироваться при необходимости при создании защищаемого ресурса.

Требования к паролям.

Минимальная длина пароля пользователя ИС должна определяться уровнем важности информации, обрабатываемой в ИС.

Минимальная длина пароля доступа к защищаемому ресурсу ИС должна определяться уровнем важности этого ресурса. При этом длина пароля не должна быть менее восьми символов;

Пароль должен включать в себя символы как минимум трех различных типов (например, цифры и буквы верхнего и нижнего регистра);

Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т. д.), а также общепринятые сокращения и любые другие данные, которые можно определить исходя из информации о пользователе (даты рождения родственников, клички домашних животных и т. д.);

Пароль не должен включать в себя последовательности из более чем 2 символов, расположенных рядом на клавиатуре (например, 123, qwe и т. д.);

Пароль не должен состоять из одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов (222999, psqpsq, и т. д.);

Правила использования паролей.

При использовании паролей пользователь обязан соблюдать положения должностных инструкций, нормативно-методических документов по защите информации, а также данной Политики;

Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

При вводе паролей необходимо исключить возможность его просмотра посторонними лицами или техническими средствами (фото видеокамеры и т. д.);

Пользователь не имеет права сообщать личный пароль другим пользователям и допускать их к работе в своей учетной записи в ИС;

Учетная запись должна блокироваться после 5 неверных попыток доступа не менее чем на 15 минут.

Запрещается использовать функции «***Запомнить пароль***» в любом программном обеспечении.

При утере, компрометации, несанкционированном изменении паролей пользователь обязан своевременно сообщать специалисту, ответственному за защиту информации в Учреждении.

Правила хранения паролей.

При хранении паролей должны быть приняты все возможные меры по минимизации возможности компрометации либо утери пароля;

Запрещается записывать пароли в файлах, электронных записных книжках, других электронных носителях информации;

Запрещается указывать пароли на бумажных и других материальных носителях информации, в том числе на предметах;

Хранение сотрудником паролей на материальном либо электронном носителе допускается только в личном сейфе владельца пароля, либо в сейфе у руководителя. При этом должны быть приняты меры, препятствующие компрометации пароля другими лицами (например, хранение в пенале, опечатанном личной печатью пользователя).

Правила смены паролей.

Плановая смена паролей пользователя должна производиться регулярно и не реже указанных в данном пункте сроков;

В ИС, в том числе предназначенных для обработки ПДн и государственных информационных ресурсов, плановая смена паролей пользователей должна производиться не реже 1 раза в 90 дней;

В случае компрометации либо утери пароля незамедлительно должна производиться его внеплановая смена. При этом пользователь должен обратиться к лицу, ответственному за защиту информации в учреждении.

Внеплановая смена паролей может проводиться по распоряжению ответственного за защиту информации в Учреждении после обнаружения фактов попыток НСД, компрометации пароля, либо других внештатных ситуаций;

При смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 символах;

При смене пароля новое значение не должно совпадать с 10 предыдущими значениями паролей доступа данного пользователя либо к данному информационному ресурсу.

Правила прекращения действия паролей:

Прекращение действия паролей возможно при истечении срока его действия, внеплановой смене, утере, удалении учетной записи, удалении защищаемого ресурса;

В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) в обязательном порядке производится удаление его учетной записи и пароля немедленно после окончания последнего сеанса работы данного пользователя с системой.

Не допускается сохранение учетных записей и паролей при окончании или прекращении полномочий связанных с ними пользователей и передача учетных записей другим пользователям;

Не допускается разглашение паролей после прекращения их действия. Повседневный контроль действий пользователей и обслуживающего персонала при работе с паролями, их смене, хранении возлагается на специалиста по обеспечению безопасности ИС, назначенного приказом по Учреждению.

Периодический контроль соблюдения информационной безопасности в учреждении при работе с паролями, их смене, хранении возлагается на лицо, ответственное за обеспечение защиты информации.

Лица, участвующие в процессах управления паролями, описанными в данной Политике, несут ответственность за надлежащее выполнение возлагаемых на них функциональных обязанностей в соответствии с законодательством Российской Федерации и внутренними локальными актами Учреждения.

Заключительные положения

Настоящая Политика является внутренним документом Учреждения, общедоступной и подлежит размещению на официальном сайте Учреждения.

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов, но не реже одного раза в три года.

При внесении изменений в актуальной редакции указывается дата последнего обновления.

Новая редакция Политики вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики.

Повседневный контроль действий пользователей и обслуживающего персонала при работе с паролями, их смене, хранении возлагается на лицо, ответственное за обеспечение защиты информации в Учреждении.

Периодический контроль соблюдения информационной безопасности в Учреждении при работе с паролями, их смене, хранении возлагается на лицо, ответственное за обеспечение защиты информации в Учреждении.

Ответственность должностных лиц Учреждения за невыполнение требований, норм, регулирующих информационную безопасность, определяется в соответствии с законодательством Российской Федерации и внутренними локальными актами Учреждения.