Приложение \_\_

к приказу № \_\_\_\_\_\_

ГБОУ СО «Алапаевская школа»

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2022 г.

**ИНСТРУКЦИЯ**

**по парольной защите информации**

**в ГБОУ СО «Алапаевская школа»**

1. **Термины и определения**
2. Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.
3. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
4. 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.
5. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
6. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
7. Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.
8. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.
9. **Общие положения**
10. Настоящая Инструкция по парольной защите информации в **ГБОУ СО «Алапаевская школа»** (далее – Инструкция) устанавливает требования и ответственность при организации парольной защиты информации, а также определяет порядок контроля за действиями пользователей и обслуживающего персонала информационных систем персональных данных (далее – ИСПДн) при работе с паролями.
11. Требования настоящей Инструкции являются обязательными для исполнения всеми пользователями и администраторами ИСПДн ГБОУ СО «Алапаевская школа» (далее – Учреждение), использующими в своей работе средства вычислительной техники.
12. Все пользователи и администраторы ИСПДн Учреждения, использующие в своей работе средства вычислительной техники, должны быть ознакомлены с требованиями настоящей Инструкции под подпись.
13. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований.
14. **Требования, предъявляемые к идентификаторам (кодам) и паролям (порядок формирования и обращения с ними)**
15. Авторизация пользователей ИСПДн осуществляется путем ввода идентификатора и/или пароля.
16. Требования к формированию паролей и обращению с ними.
17. Пароль формируется при создании учетной записи ответственным обеспечение безопасности ПДн в ИСПДн или администратором ИСПДн, при первичном входе в учетную запись пароль должен быть изменен владельцем.
18. Владельцы личных паролей обязаны обеспечить их тайну.
19. Пароли генерируются с учетом следующих требований:
* пароль должен знать только его владелец;
* длина пароля должна быть не менее 8 символов;
* в пароле обязательно должны присутствовать как цифры, так и буквы на верхнем и нижнем регистрах;
* пароль не должен включать смысловую нагрузку (имена, фамилии, наименования организаций, улиц, городов и т.д.), общепринятые сокращения (userOl, password02 и т.п.) и последовательные сочетания клавиш клавиатуры (qwertyOl, Ицукен12);
* максимальный срок действия пароля составляет 120 дней;
* минимальный срок действия пароля составляет 2 дня;
* количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя должно быть не более 6.
1. Требования к формированию паролей обеспечиваются техническими возможностями используемых операционных систем, средств защиты информации и информационных ресурсов.
2. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода. Внеплановая смена пароля производится в случае его компрометации, а также по просьбе пользователя ИСПДн.
3. Хранение пользователями ИСПДн значений своих паролей на бумажном носителе ЗАПРЕЩЕНО.
4. Пользователь не имеет права сообщить личный пароль другим лицам (разрешается только с согласования ответственного за обеспечение безопасности или администратора ИСПДн при наличии технологической необходимости использования имен и паролей работников в их отсутствие в случае возникновения нештат6ных ситуаций, форс-мажорных обстоятельств и т.п. По возращению работники обязаны сразу же сменить свои пароли на новые значения согласно данной Инструкции).
5. Порядок смены паролей и идентификаторов при изменениях в организационно-штатной структуре (кадровые перестановки, увольнение работников):
6. При прекращении действия трудового договора с работником все созданные для этого работника учетные записи (пользовательское имя) подлежат блокированию не позднее, чем в день увольнения работника. Полное удаление учетных записей производится в течении 5 рабочих дней со дня увольнения работника. Основанием для блокирования и последующего удаления учетных записей работника является заявка, представленная непосредственным руководителем увольняемого не позднее, чем за 3 рабочих дня до дня его увольнения.
7. При проведении организационно-штатных мероприятий (кадровые перестановки) непосредственный руководитель структурного подразделения обязан представить администратору ИСПДн заявку на изменение в правах доступа.
8. Порядок действий при компрометации идентификаторов и паролей.
9. Под компрометацией понимается: утрата пароля учетной записи и (или) пароля идентификатора, разглашение учетной записи пароля или пароля идентификатора (явная компрометация), или иная ситуация, которая дает основание для предположения о нарушении конфиденциальности паролей и идентификаторов (неявная компрометация).
10. При выявлении факта утраты пароля, разглашения пароля, пароля идентификатора, самого идентификатора пользователь обязан незамедлительно сообщить о данных фактах своему непосредственному руководителю и ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн.
11. В случае выявления факта компрометации идентификаторов и паролей пользователя администратор ИСПДн или ответственный за обеспечение безопасности ПДн в ИСПДн обязан немедленно заблокировать учетную запись данного пользователя и незамедлительно произвести внеплановую смену пароля для этого пользователя.
12. **Права и обязанности**
13. Основные задачи администратора ИСПДн:
* организация установки средств идентификации и аутентификации;
* организация парольной защиты во всех ИСПДн;
* выдача первичных паролей, и электронных персональных идентификаторов и паролей к ним;
* осуществление контроля за состоянием системы парольной защиты информации в ИСПДн.
1. Администратор ИСПДн имеет право:
* вносить предложения по совершенствованию системы парольной защиты информации в ИСПДн;
* принимать участие в планировании мероприятий по парольной защите информации в ИСПДн и планировании оснащения средствами идентификации и аутентификации;
* осуществлять контроль состояния средств идентификации и аутентификации в ИСПДн;
* инициировать служебные проверки и участвовать в проведении расследований по фактам компрометации;
* оказывать помощь в решении проблем, возникающих при эксплуатации средств идентификации и аутентификации.
1. Обязанности в части парольной защиты информации отражены в инструкции администратора ИСПДн.
2. Пользователям ИСПДн в своей работе запрещается:
* сообщать кому-либо свой личный пароль и/или пароль к электронному персональному идентификатору;
* передавать кому-либо выданный электронный персональный идентификатор;
* осуществлять вход в операционные системы ИСПДн и в информационные ресурсы под чужими идентификаторами и паролями;
* отключать средства идентификации и аутентификации.
1. В случае появления подозрений на факт компрометации пароля, а также в случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств идентификации и аутентификации, пользователи обязаны немедленно проинформировать об этом ответственного за обеспечение безопасности ПДн в ИСПДн или администратора ИСПДн.
2. **Ответственность должностных лиц в рамках системы парольной защиты информации**
3. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.
4. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.
5. **Срок действия и порядок внесения изменений**
6. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.
7. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.
8. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.