УТВЕРЖДЕНА
приказом директора ГУСО
«Хохотуйский центр помощи детям,
оставшимся без попечения родителей
«Берёзка» Забайкальского края
от «08» мая 2024 года № 278

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем Государственного учреждения социального обслуживания «Хохотуйский центр помощи детям, оставшимся без попечения родителей «Берёзка» Забайкальского края

с. Хохотуй
2024

I. Назначение

1.1. Настоящая Инструкция по организации парольной защиты информационных систем Государственного учреждения социального обслуживания «Хохотуйский центр помощи детям, оставшимся без попечения родителей «Берёзка» Забайкальского края (далее – Инструкция, Учреждение соответственно) регламентирует организационно - техническое обеспечение процессов генерации, смены и прекращения действия паролей пользователей в информационных системах, а также контроль за действиями пользователей и обслуживающего персонала при работе с паролями.

II. Область применения

2.1. Настоящая Инструкция применяется пользователями любых информационных систем, используемых в работе Учреждения.

III. Нормативные ссылки

3.1. Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства РФ от 01.11.2012 № 1119;
- Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17 (Зарегистрировано в Минюсте России 31.05.2013 №28608);
- Специальными требованиями и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282;
- Методическим документом «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

IV. Термины, обозначения и сокращения

4.1. В настоящей Инструкции используются следующие термины и определения:

4.1.1. **Администратор безопасности информации** - лицо, отвечающее за защиту автоматизированных систем от несанкционированного доступа к информации, за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации

4.1.2. **Безопасность информации [данных]** - 1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность; 2) состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

4.1.3. **Идентификатор пользователя** - символьное или цифровое имя, присваиваемое отдельному лицу или группе лиц и разрешающее использование ресурсов информационной системы.

4.1.4. **Информационная система (ИС)** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

4.1.5. **Информационная система персональных данных (ИСПДн)**- совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

4.1.6. **Пароль** – 1) наиболее распространенные средства подтверждения идентификатора пользователя при доступе к информационной системе или сервису; 2) конфиденциальная аутентификационная информация, обычно состоящая из строки знаков.

4.1.7. **Пользователь (потребитель) информации** – 1) субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею; 2) сотрудник Министерства, допущенный в установленном порядке к работе с конфиденциальной информацией, полномочия которого регламентированы внутренними организационно- распорядительными актами.

4.1.8. **Регуляторы** - Федеральная служба по техническому и экспортному контролю (ФСТЭК России), Федеральная служба безопасности (ФСБ России), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

4.2. В настоящей Инструкции используются следующие сокращения:

4.2.1. **АС** – автоматизированная система;

4.2.2. **ГИС**- государственная информационная система (в тексте настоящей Инструкции под ГИС понимаются ГИС «ППО АИСТ ГБД» и ГИС «АС «АСП»);

4.2.3. **ИС** – информационная система;

4.2.4. **ИСПДн** - информационная система персональных данных;

4.2.5. **ПДн** – персональные данные;

4.2.6. **ПЭВМ** – персональная электронно - вычислительная машина;

4.2.7. **СЗИИС** – система защиты информации информационных систем.

V. Общие положения

5.1. Организация парольной защиты возложена на администратора безопасности информации.

5.1.1. Администратор безопасности информации обязан регулярно докладывать руководителю Учреждения, ответственного за организацию обеспечения безопасности информации в информационных системах Учреждения, служебной запиской о результатах периодической проверки состояния парольной защиты внутренних пользователей в ИС.

VI. Требования к генерации, использованию, смене и прекращении действия паролей

6.1. В целях разграничения доступа к информационным ресурсам информационных систем устанавливаются единые требования к генерации, использованию, смене и прекращении действия паролей.

6.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей пользователей в информационных системах возлагается на администратора безопасности информации.

6.3. Авторизация и аутентификация в информационных системах осуществляется при помощи имени пользователя и пароля, вводимого с клавиатуры, или электронного ключевого носителя (далее – электронный ключ).

6.4. Аутентификация по электронному ключу осуществляется по хранимому на нем сертификату электронной цифровой подписи (ЭЦП) или паролю.

6.5. В Учреждении установлены заданные характеристики паролей, так каждый пароль должен выбираться и генерироваться пользователем с учетом следующих требований:

а) длина пароля не менее шести символов, алфавит пароля не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут, смена паролей не более чем через 180 дней;

6.6. В информационных системах должен использоваться механизм одноразовых паролей при аутентификации пользователей, осуществляющих удаленный или локальный доступ.

6.7. В информационных системах должно быть обеспечено использование автоматизированных средств для формирования аутентификационной информации (генераторов паролей) с требуемыми характеристиками стойкости (силы) механизма аутентификации и для оценки характеристик этих механизмов.

6.8. В информационных системах должно обеспечиваться противодействие автоматизированному подбору паролей с использованием однократных кодов, требующих визуального распознавания.

6.9. Пользователь не имеет права сообщать никому личный пароль. Системный администратор не имеет права разглашать личный пароль и пароли на доступ к системам управления ИС.

6.10. Запрещается запись паролей на бумаге, если только не обеспечено безопасное их хранение.

6.11. Пользователям запрещается использование их идентификаторов и паролей в других информационных системах.

6.12. Владельцы паролей должны быть ознакомлены под подпись с перечисленными выше требованиями и предупреждены о дисциплинарной ответственности за использование паролей, не соответствующих указанным требованиям, а также за разглашение парольной информации.

6.13. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на программиста.

6.14. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

6.15. Внеплановая смена личного пароля в случае прекращения полномочий работника должна производиться программистом немедленно после окончания последнего сеанса работы данного пользователя с ИС.

6.16. Внеплановая смена всех паролей внутренних пользователей информационных систем должна проводиться в случае компрометации пароля (потери электронного ключа) администратором безопасности информации (программистом).

6.17. При увольнении или перемещении администратора безопасности информации (программиста) руководителем Учреждения, ответственного за организацию обеспечения безопасности информации в информационных системах Учреждения должны быть приняты меры по оперативному изменению паролей, идентификаторов и ключей шифрования.

6.18. В случае компрометации личного пароля внутреннего пользователя ИС должны быть немедленно предприняты меры в соответствии с п.6.16 и п.6.17 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

6.19. Повседневный контроль за действиями внутренних пользователей и обслуживающего персонала ИС при работе с паролями, соблюдением правил их смены, хранения и использования возлагается на администратора безопасности информации (программиста). После предоставления текущего значения пароля для проверки на соответствие установленным требованиям контролируемый пользователь обязан сменить свой пароль.

VII. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

7.1. В информационных системах должны выполняться следующие требования Регуляторов к реализации контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе:

7.1.1. Администратором безопасности информации (программистом) должен проводиться контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

7.1.2. При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

- контроль правил генерации и смены паролей пользователей в соответствии с требованиями Регуляторов;
- контроль заведения и удаления учетных записей пользователей в соответствии с требованиями Регуляторов;
- контроль реализации правил разграничения доступом в соответствии с требованиями Регуляторов;
- контроль реализации полномочий пользователей в соответствии с требованиями Регуляторов;
- контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации оператора;
- устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

7.1.3. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе проводится администратором безопасности информации (программистом) не реже одного раза в месяц.

7.2. Администратором безопасности информации (программистом) должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей,

реализации правил разграничения доступом, полномочий пользователей в информационных системах:

7.2.1. В информационных системах должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей.

7.2.2. Оператором должны использоваться автоматизированные средства, обеспечивающие контроль правил генерации и смены паролей пользователей, учетных записей пользователей, правил разграничения доступом и полномочий пользователей.

VIII. Ответственность и полномочия персонала

8.1. Ответственность персонала

8.1.1. За нарушение требований настоящей Инструкции должностные лица Учреждения несут ответственность в соответствии с действующим законодательством.

8.2. Полномочия персонала

8.2.1. Сотрудники Учреждения имеют право выходить с предложениями к руководителю Учреждения по вопросам защиты конфиденциальной информации.

IX. Заключительные положения

9.1. Изменения в настоящую Инструкцию вносятся приказом Учреждения после обязательного согласования вносимых изменений с ответственным за организацию обработки персональных данных в Учреждении, ответственного за организацию обеспечения безопасности информации в информационных системах Учреждения, отвечающими за соответствие вносимых изменений требованиям законодательства и нормативно- правовых актов Регуляторов.

9.2. Положения настоящей Инструкции применяются совместно с положениями Инструкции по криптографической защите и обращению со средствами криптографической защиты в Государственном учреждении социального обслуживания «Хохотуйский центр помощи детям, оставшимся без попечения родителей «Берёзка» Забайкальского края, утвержденным приказом Учреждения от 08 мая 2024 года №272 (далее – Инструкция).

9.3. Положения настоящей Инструкции имеют приоритет над положениями указанной Инструкции.