Приложение № 4

Утверждено

приказом государственной

инспекции по охране объектов

культурного наследия

Новосибирской области

от \_\_\_\_\_\_ 2023 г. № \_\_\_\_\_

Инструкция

по организации парольной защиты в информационных системах персональных данных

1. Общие положения

1.1. Настоящая Инструкция по организации парольной защиты в информационных системах персональных данных (далее – Инструкция) определяет порядок использования, генерации, смены и прекращения действия паролей пользователей в информационных системах персональных данных (далее – ИСПДн), а также контроль действий пользователей при работе с паролями. Инструкция распространяется на все ИСПДн, существующие и вновь создаваемые в ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности их работы.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль за реализацией требований по обеспечению безопасности при использовании паролей возлагается на администратора безопасности информации.

2. Требования к организации парольной защиты

2.1. Установку первичного пароля производит администратор безопасности информации при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на администраторе безопасности информации.

2.2. При создании первичного пароля, администратор безопасности информации обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

2.3. Первичный пароль так же используется при сбросе забытого пароля на учетную запись.

2.4. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

2.5. Устанавливаемые пароли должен отвечать следующим требованиям:

длина пароля должна быть не менее 8 символов;

пароль должен содержать строчные и прописные буквы, а также небуквенные символы (цифры, знаки пунктуации, специальные символы);

пароль, должен отличаться от предыдущего не менее чем на 4 символа;

использование трех и более, подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;

использование в качестве пароля одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов недопустимо;

новое значение пароля не должно совпадать с одним из пяти предыдущих значений;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования автоматизированного рабочего места, имя учетной записи или какую-либо его часть, общепринятые сокращения (password, USER, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе.

2.6. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом администратору безопасности информации и изменить основной пароль.

2.7. Восстановление забытого основного пароля пользователя осуществляется администратором безопасности информации путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной либо электронной заявки пользователя.

2.8. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

2.9. Для предотвращения несанкционированного доступа в ИСПДн должен быть реализован механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

2.10. Разблокирование учетной записи пользователя осуществляется администратором безопасности информации на основании заявки владельца учетной записи.

2.11. Должен быть установлен пароль на доступ к настройкам используемых средств защиты информации. Указанный пароль должен отвечать установленным требованиям (п. 2.5.).

2.12. Пользователи и администратор безопасности информации обязаны:

сохранять в тайне свой личный пароль;

четко знать и строго выполнять требования настоящей Инструкции;

своевременно сообщать лицам, ответственным за обеспечение безопасности ПДн обо всех нештатных ситуациях, нарушениях работы подсистем защиты от несанкционированного доступа, возникающих при работе с паролями.

2.13. При организации парольной защиты запрещается:

записывать свои пароли на любой носитель;

хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги;

сообщать посторонним лицам, в том числе сотрудникам ГИО ОКН НСО безопасности информации, свои пароли, а также пересылать открытым текстом в электронных сообщениях.

3. Порядок применения парольной защиты

3.1. Полная плановая смена паролей производится регулярно, не реже одного раза в 90 дней. При плановой смене пароля, пользователь самостоятельно меняет свой пароль.

3.2. Внеплановая смена (удаление) личного пароля любого пользователя производится в следующих случаях:

по окончании срока действия пароля;

в случае прекращения полномочий пользователя;

при обнаружении факта успешной попытки несанкционированного доступа к элементам ИСПДн;

при обнаружении факта компрометации пароля.

3.3. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности информации.

3.4. Скомпрометированные пароли выводятся из действия немедленно.

3.5. Порядок внеплановой смены пароля аналогичен порядку плановой смены пароля.

3.6. По каждому случаю, связанному с компрометацией действующих паролей, ответственным за обеспечение безопасности персональных данных, организуется и проводится служебное расследование.

3.7. Результаты служебного расследования в виде служебной записки предоставляются руководителю структурного подразделения или ответственному за организацию обработки персональных данных. По результатам расследования лица, допустившие разглашение паролей, привлекаются к дисциплинарной ответственности.