Приложение 6
Утверждены
постановлением Администрации
Ребрихинского района Алтайского края

от 28.12.2018 №745

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах Администрации Ребрихинского района Алтайского края

1. Общие положения

1.1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах Администрации Ребрихинского района Алтайского края (далее – «ИС»), а также контроль за действиями пользователей и обслуживающего персонала ИС при работе с парольной защитой.

1.2. Идентификация и аутентификация пользователей в ИС осуществляется посредством использования персональных учетных записей пользователей ИС и периодически сменяемых паролей. Пароли пользователей ИС должны содержать не менее шести символов, состоять из букв и цифр, а также при смене пароля отличаться от прежнего минимум на 3 символа. Обязательная реализация идентификации и аутентификации реализуется в рамках домена вычислительной сети Администрации Ребрихинского района Алтайского края (далее – «организация») на автоматической основе, дополнительно реализуется программным обеспечением ИС.

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС, а также контроль за действиями пользователей и обслуживающего персонала ИС при работе с паролями возлагается на начальника одела информатизации района Алтайского края (далее- администратора безопасности ИС).

1.4. Временный пароль, задаваемый при создании учетной записи или смене забытого пароля, должен передаваться способом, исключающим доступ к нему других лиц, и быть изменен пользователем при первом обращении к ИС. Пароли, предустановленные производителем программного обеспечения, средства защиты информации и т.д. должны изменяться до начала их эксплуатации.

2. Порядок генерации, смены и прекращения действия и резервирования паролей

2.1. В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам ИС пользователями осуществляется периодическая (не реже раза в шесть месяцев) замена пароля в автоматическом режиме в домене вычислительной сети и по возможности в другом программном обеспечении ИС. Замена пароля осуществляется

пользователем ИС самостоятельно или с привлечением администратора безопасности ИС.

2.2. В случае прекращения полномочий пользователя ИС (увольнение, переход на другую работу и т.п.) подразделение или лицо, ответственное за кадровое обеспечение организации должно уведомить об этом администратора безопасности ИС.

Администратор безопасности ИС должен произвести блокирование или удаление учетной записи пользователя ИС незамедлительно после получения такого уведомления.

2.3. Внеплановая смена паролей всех пользователей ИС должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности ИС и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

2.4. В случае компрометации личного пароля пользователя ИС проводится внеплановая смена пароля, которая выполняется лично или администратором безопасности ИС устанавливается временный пароль.

2.5. Повседневный контроль за действиями пользователей и обслуживающего персонала ИС при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей структурных подразделений организации, администратора безопасности ИС, периодический контроль - возлагается на руководителя подразделения или лицо, ответственное за организацию обработки информации.

2.6. По решению руководителя структурного подразделения, может применяться резервирование паролей ключевых пользователей, таких, как администратор безопасности ИС, отдельных пользователей, выполняющих ключевые функции, а также пользователей, обеспечивающих работу отдельных сетевых сервисов.

2.7. Для резервирования пароля выполняются следующие действия:

пароль записывается на лист бумаги;

лист с записью пароля вкладывается владельцем в конверт. Конверт не должен допускать просмотр записи пароля на просвет. Если конверт недостаточно плотный, в него может быть вложен лист темной бумаги. Конверт заклеивается, при необходимости - опечатывается;

на конверте владелец пароля указывает свою должность, фамилию и инициалы, наименование информационного средства, доступ к которому защищается этим паролем, текущую дату и время, при необходимости – другие данные, и заверяет запись личной подписью;

конверт передается на хранение руководителю структурного подразделения или лицу, им для этого назначенным;

конверты с паролями хранятся у руководителей структурных подразделений или у администратора безопасности ИС в условиях, исключающих бесконтрольный доступ к ним. Указанные должностные лица обязаны проверять наличие конвертов с паролями, не реже раза в квартал;

при замене пароля конверт передается владельцу пароля, который уничтожает лист с резервным паролем. Новый резервный пароль

подготавливается к хранению так, как указано выше;

вскрытие конверта с паролем производится по решению руководителя структурного подразделения в случае необходимости использования прав доступа его владельца в отсутствие самого владельца. О вскрытии конверта составляется акт, утверждаемый руководителем подразделения, который по окончании работы хранится в деле подразделения;

при появлении владельца пароля, после факта вскрытия конверта, пароль заменяется на новый и вновь сохраняется его копия, как описано выше.

3. Запрещается:

сообщать свой пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых пользователей ИС);

сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

использовать учетные записи других лиц.