Утверждено
Приказом и.о.генерального директора
Фонда капитального ремонта ВО
от 18.12.2018 № 110/3

ИНСТРУКЦИЯ
по применению парольной политики в информационной системе персональных данных

1. Общие положения

Настоящая Инструкция устанавливает порядок работы пользователей информационных систем персональных данных (ИСПДн) некоммерческой организации «Фонд капитального ремонта многоквартирных домов Владимирской области» (далее по тексту - Фонд) со своими учетными записями и паролями доступа и правила парольной политики, направленной на обеспечение безопасности ПДн.

Основной целью Инструкции является установление правил парольной политики для пользователей ИСПДн.

2. Общие требования

Пароли для всех учетных записей пользователей ИСПДн, должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы и цифры;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования АРМ, организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);
- пароль должен легко запоминаться, для этого используются некоторые приемы, например: для задания пароля используется четверостишье: «ваше благородие, госпожа удача, для кого вы добрая, для кого иначе», далее для пароля берут первые буквы «вбгудквддки» и в конце добавляется число символов – 11, таким образом, получаем пароль – вбгудквддки11;
- минимальное время применения пароля - не менее 2 дней;
- максимальное время применения пароля - не более чем 60 дней;
- пароль не должен повторяться;
- пользователь не может неправильно ввести пароль учетной записи более 3 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки системным администратором, обслуживающим программы обработки персональных данных.

Смена пароля учетной записи пользователя должна проводиться регулярно и не реже одного раза в квартал.

В случае прекращения полномочий учетной записи пользователя (увольнение, переход на другую работу, в другой отдел или помещение, а также и другие

обстоятельства) учетная запись должна быть заблокирована и пароль должен быть заменен сразу после окончания последнего сеанса работы данного пользователя в ИСПДн. Удалять учетную запись не рекомендуется, с целью возможной необходимости просмотра «лог-файлов» по данной учетной записи.

3. Требования к владельцам паролей

Пользователи обязаны хранить свой личный пароль втайне от других и не передавать любым способом пароль никому.

Хранение пользователем значений своих паролей на бумажном носителе допускается только в запираемых ящиках столов, сейфах или других труднодоступных местах. Хранение бумажных носителей паролей в доступных местах (под клавиатурой, на мониторе и т.д.) категорически запрещено.

В случае компрометации личного пароля пользователь ИСПДн должен немедленно предпринять меры, указанные в п.4 настоящей Инструкции.

4. Компрометация паролей

Пользователь при компрометации или подозрении на компрометацию своего пароля, утере личного идентификатора обязан без промедления сообщить об этом ответственному за организацию обработки ПДн в устной форме.

Ответственный за организацию обработки ПДн должен провести следующие мероприятия:

– взять объяснительную в письменном виде с пользователя, обнаружившего компрометацию пароля. Объяснительная пишется на имя руководителя и должна содержать ФИО, должность пользователя, описание обстоятельств, при которых была обнаружена компрометация, утеря личного идентификатора или описание причин подозрения на компрометацию, последние действия, проведенные в автоматизированной системе, личную подпись пользователя;

– запросить у начальника отдела информационно-технического обеспечения внеочередную смену пароля пользователя или при утере личного идентификатора блокировку учетной записи пользователя, для предотвращения использования злоумышленником данной учетной записи;

– запросить у начальника отдела информационно-технического обеспечению журнал операций в автоматизированной системе по пользователю ИСПДн и проанализировать его;

– в случае выявления действий, не указанных пользователем в объяснительной, проводится служебное расследование по выяснению причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины нанесенного ущерба безопасности информации;

– в случае не обнаружения никаких признаков использования пароля или идентификатора пользователя в несанкционированных целях, составляется Акт об отсутствии нарушений при использовании пароля. К Акту подшивается объяснительная пользователя;

– акты и документы по служебным расследованиям хранятся у ответственного за организацию обработки ПДн в течение двух лет, затем подлежат уничтожению.

5. Проверка соблюдения парольной политики

Начальником отдела информационно-технического обеспечения, проводится периодическая проверка выполнения пользователями ИСПДн парольной политики в соответствии с Планом внутренних проверок условий обработки персональных данных.

Проверка проводится на местах. Количество проверяемых пользователей и периодичность проверки определяется начальником отдела информационно-технического обеспечению самостоятельно.

В ходе проверки проверяется знание пользователями парольной политики и места хранения бумажных носителей паролей, а так же периодичность смены пароля, если эта функция не выполняется в автоматическом режиме.

Результаты проверки фиксируются в Протоколе проведения внутренней проверки.

В случае выявления нарушений к пользователю могут быть применены меры наказания, на усмотрение руководителя.