Приложение № 19
к приказу Директора МБОУ СОШ д.Султанбеково
МР Аскинский район РБ
от «21» 11 2018 г. № 88 од

Положение

по организации парольной защиты

1. Общие положения

1.1. Настоящее Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей, а также контроль за действиями пользователей информационных систем персональных данных (далее – Пользователь) при работе с паролями в МБОУ СОШ д.Султанбеково МР Аскинский район РБ (далее – Оператор).

1.2. Положение распространяется на всех Пользователей и информационные системы персональных данных (далее – ИСПДн) Оператора.

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в системном и прикладном программном обеспечении, средствах защиты информации, серверном и сетевом оборудовании входящих в ИСПДн (далее – компоненты ИСПДн) возлагается на Ответственного за обеспечение безопасности персональных данных.

1.4. Повседневный контроль за действиями при работе с паролями, соблюдением правил их хранения и использования возлагается на Ответственного за за обеспечение безопасности персональных данных.

2. Определения

2.1 Системное программное обеспечение – комплекс программ, которые обеспечивают управление компонентами компьютерной системы, такими как процессор, оперативная память, устройства ввода-вывода, сетевое оборудование, выступая как «межслойный интерфейс», с одной стороны которого аппаратура, а с другой — приложения Пользователя (BIOS, операционные системы, утилиты, системы программирования, системы управления базами данных, связующее программное обеспечение).

2.2 Прикладное программное обеспечение - программа, предназначенная для выполнения определённых задач и рассчитанная на непосредственное взаимодействие с Пользователем.

3. Порядок создания паролей

3.1. Пароли доступа создаются на всех компонентах ИСПДн, имеющих механизмы идентификации и аутентификации.

3.2. Создание паролей доступа осуществляется Ответственным за обеспечение безопасности ИСПДн.

3.3. При заведении нового Пользователя для него должен быть назначен логин и однократный пароль.

3.4. Пользователь обязан заменить однократный пароль – личным при первом же подключении к защищаемому ресурсу ИСПДн.

3.5. При отсутствии возможности создания однократного пароля, с последующей сменой Пользователем, создается постоянный пароль.

3.6. Одноразовый пароль может передаваться Пользователю лично на бумажном носителе, в электронном виде на адрес индивидуальной рабочей электронной почты или в устной форме.

3.7. Постоянный пароль передается Пользователю в запечатанном конверте.

3.8. Пользователь обязан хранить в тайне пароль и любые другие средства доступа к информационным ресурсам.

3.9. Пароли от учетных записей, обладающих правами Администратора, могут выдаваться только лицам, осуществляющим администрирование ИСПДн. Выдачу паролей учетных записей, обладающих правами Администратора, осуществляет Ответственный за обеспечение безопасности персональных данных.

4. Период действия паролей

4.1. Периодичность смены паролей для программного обеспечения составляет 12 месяцев.

4.2. При сообщении программного обеспечения об окончании срока действия пароля Пользователь обязан заменить его на новый, ранее не применявшийся.

4.3. Смена паролей в программном обеспечении, не имеющем функционал установления срока действия пароля, осуществляется лицом, осуществляющим администрирование ИСПДн в соответствие с установленной периодичностью.

4.4. Внеплановая смена пароля или блокирование учетных записей Пользователя в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться в течение двух рабочих часов после получения копии приказа о прекращении полномочий.

4.5. Внеплановая полная смена паролей учетных записей, обладающих правами Администратора должна производиться в случае прекращения полномочий (увольнение, переход на другую работу, окончание действия договора на обслуживание и другие обстоятельства) лица, осуществляющего администрирование ИСПДн.

5. Конфиденциальность паролей

5.1. Информация о персональных паролях Пользователей является конфиденциальной информацией и разглашению не подлежит.

5.2. Пользователи несут ответственность за сохранность выбранного самостоятельно постоянного пароля, и за действия, совершаемые под выданной Пользователю учетной записью.

5.3. Компоненты ИСПДн должны быть настроены таким образом, чтобы исключить возможность ознакомления Пользователей и Администраторов с действующими и истекшими паролями.

6. Принципы выбора и формирования личных паролей

6.1. Одноразовые и постоянные пароли для доступа к компонентам ИСПДн должны соответствовать следующим требованиям:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

6.2. При наличии такой возможности, системы аутентификации прикладного программного обеспечения должны обеспечивать выше обозначенные требования к сложности пароля.

6.3. Рекомендуется в виде пароля выбирать последовательности типа "X0Posh6" "!1рыБ@lkA" или "Def*en$6"

6.4. При смене пароля запрещается использовать ранее использованные пароли, а новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

6.5. Выбор паролей на учетных записях Администратора осуществляется по тем же требованиям, за исключением длина пароля – она должна быть не менее 8 символов.

7. Правила использования и сохранения в тайне личного пароля

7.1. Пароли необходимо запомнить. Допускается хранение паролей в индивидуальных сейфах и опечатываемых шкафах.

7.2. В случае подозрения на компрометацию пароля, сотрудники обязаны произвести экстренную замену личного пароля, при наличии такого права, и незамедлительно поставить об этом в известность Ответственного за обеспечение безопасности ПДн для исключения возможности утечки информации.

7.3. Ответственный за обеспечение безопасности ПДн обязан произвести расследование причин компрометации пароля.

7.4. Типовые случаи компрометации пароля:

- файлы, хранящиеся в ИСПДн, были несанкционированно изменены;
- изменено расположение иконок программ и файлов на рабочем столе АРМ и личных папках;
- при правильном вводе пароля выдается ошибка доступа;
- другие сотрудники знают ваш пароль.

8. Ответственность

8.1. За невыполнение требований настоящего Положения применяется дисциплинарная ответственность в порядке, определенным трудовым кодексом Российской Федерации и локальными актами Оператора.