«Утверждено»
приказом заведующей
МБДОУ «Детский сад № 3 посёлка Домново»

_____ Н.Н.Верба

Инструкция по организации парольной защиты

1. Общие положения

1.1. Настоящий документ разработан в соответствии с 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», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее - ИСПД) МБДОУ «Детский сад № 3 поселка Домново» (далее - Учреждение), а также контроль над действиями пользователей и обслуживающего работника системы при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПД и контроль над действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ИСПД.

2. Правила формирования паролей

2.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационной системы самостоятельно с учётом следующих требований:

- 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 имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

2.2. Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Ротлвцф9?).

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

2.4. Для обеспечения возможности использования имён и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учётных записей инженеру-программисту ИСПДн в запечатанном конверте или опечатанном пенале. Опечатанные конверты (пеналы) с паролями работников должны храниться в опечатанном сейфе, к которому исключен доступ других работников Учреждения и посторонних лиц. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии), либо печать инженера- программиста ИСПДн. Все конверты (пеналы) с паролями в обязательном порядке фиксируются в «Журнале учёта паролей пользователей...».

3. Ввод пароля

3.1. При вводе пароля работнику необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).
3.2. При неверном вводе пароля более 5 раз, учётная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

4. Порядок смены личных паролей

4.1. Смена паролей должна проводиться регулярно, не реже одного раза в 6 месяцев, самостоятельно каждым пользователем.
4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.
4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за обеспечение безопасности персональных данных, инженера-программиста и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.
4.4. Администратор безопасности ИСПД ведет «Журнал учёта паролей пользователей...», в котором он отмечает причины внеплановой смены паролей пользователей.
4.5. Временный пароль, заданный администратором безопасности ИСПД при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

5. Хранение паролей

5.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах, и носителях информации.
5.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.
5.3. Запрещается регистрировать других пользователей в ИСПД со своим личным паролем, запрещается входить в ИСПД под учётной записью и паролем другого пользователя.

6. Действия в случае утери и компрометации пароля

6.1.В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

7. Ответственность

7.1. Каждый пользователь ИСПД несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИСПД, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

7.2. Ответственность за контроль проведения мероприятий по организации парольной защиты в отделах возлагается на ответственного за обеспечение безопасности персональных данных заместителей заведующего Учреждения.

7.3. За разглашение персональных данных и нарушение порядка работы со средствами ИСПД, обрабатывающими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.