

# **Инструкция по организации парольной защиты**

## **1. ОБЩИЕ ПОЛОЖЕНИЯ**

**1.1.** Настоящий документ разработан в соответствии нормативными документами по безопасности информации и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) МБДОУ ДС №50 (далее – Учреждение), а также контроль над действиями пользователей и обслуживающего персонала системы при работе с паролями.

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

## **2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

**2.1. Информация** – сведения (сообщения, данные) независимо от формы их представления.

**2.2. Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

**2.3. Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**2.4. Пароль** – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

**2.5. Компрометация пароля** – раскрытие, обнаружение или утеря пароля.

## **3. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ**

**3.1.** Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационной системы самостоятельно с учетом 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.

**3.2.** Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

**3.3.** В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности ИСПДн.

**3.4.** Для обеспечения возможности использования имен и паролей некоторых работников в их отсутствие (например, в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИСПДн в запечатанном конверте или опечатанном пенале. Опечатанные конверты (пеналы) с паролями работников должны храниться в 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 администратора безопасности ИСПДн. Все конверты (пеналы) с паролями в обязательном порядке фиксируются в «Журнале учета паролей пользователей...».

#### **4. ВВОД ПАРОЛЯ**

**4.1.** При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

**4.2.** При неверном вводе пароля более 5 раз, учетная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

#### **5. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ**

**5.1.** Смена паролей должна проводиться регулярно, не реже одного раза в 12 месяцев, самостоятельно каждым пользователем.

**5.2.** 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.

**5.3.** 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, администратора безопасности и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

**5.4.** Администратор безопасности ИСПДн ведет «Журнал учета паролей пользователей...», в котором он отмечает причины внеплановой смены паролей пользователей.

**5.5.** Временный пароль, заданный администратором безопасности ИСПДн при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

## **6. ХРАНЕНИЕ ПАРОЛЯ**

**6.1.** Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других носителях информации.

**6.2.** Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

**6.3.** Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учетной записью и паролем другого пользователя.

## **7. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕТАЦИИ ПАРОЛЯ**

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

## **8. ОТВЕТСТВЕННОСТЬ**

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

**8.2.** Ответственность за контроль проведения мероприятий по организации парольной защиты в отделах возлагается на ответственного за обеспечение безопасности персональных данных.

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