

**Частное дошкольное образовательное учреждение
«РЖД детский сад № 31»**

Принято с учетом мнения
выборного органа первичной
профсоюзной организации
«РЖД детский сад №31»
Председатель профсоюзной
организации
/Кочнева С.В./
«23» сентября 2024 г.



Утверждаю:
Заведующий частным
дошкольным образовательным
учреждением
«РЖД детский сад №31»
Т.Ю. Светлакова/



Инструкция об организации парольной защиты

1. Общие положения

1.1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее – Инструкция) разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, 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», Указом Президента Российской Федерации от 06.03.1997 № 188 (в ред. от 13.07.2015) «Об утверждении перечня сведений конфиденциального характера», постановлением Правительства Российской Федерации от 15 сентября 2008 года №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными правовыми актами Российской Федерации.

1.2. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов установки, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах частного дошкольного образовательного учреждения «РЖД детский сад № 31» (далее – Учреждение).

1.3. Инструкция призвана регламентировать контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.4. Организационное и техническое обеспечение процессов установки, использования, смены и прекращения действия паролей в информационных системах Учреждения и контроль за действиями исполнителей при работе с паролями возлагается на заведующего Учреждением.

2. Правила формирования паролей

2.1. Личные пароли устанавливаются и распределяются централизованно с учетом следующих требований:

2.1.1. Пароль должен состоять не менее чем из шести символов.

2.1.2. В пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы.

2.1.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно основываясь на информации о пользователе.

2.1.4. При смене пароля новый пароль должен отличаться от старого не менее чем в четырех позициях.

2.2. Пароли пользователей регистрируются в журнале (форма указана ниже). Страницы журнала регистрации паролей пользователей нумеруются, прошиваются и скрепляются печатью и подписью заведующего Учреждением. Журнал регистрации паролей

пользователей должен храниться в сейфе ответственного за информационную безопасность –заведующего Учреждением.

2.3. При технологической необходимости смены паролей некоторых работников (исполнителей), в том числе в их отсутствие (в случае возникновения внештатных ситуаций, форс-мажорных обстоятельств и т.п.), все изменения вносятся в журнал регистрации паролей пользователей.

3. Ввод пароля

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

4. Порядок смены личных паролей

4.1. Смена паролей проводится по мере необходимости.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) ответственный за информационную безопасность -заведующий Учреждением должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с пунктом 2.1 настоящей Инструкции.

4.5. Временный пароль, заданный ответственным за информационную безопасность -заведующим Учреждением, при регистрации нового пользователя, следует изменить при первом входе в систему.

5. Хранение паролей

5.1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе заведующего Учреждением.

5.2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

5.3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. Действия в случае утери и компрометации пароля

6.1. В случае утери или компрометации пароля пользователя должны быть немедленно приняты меры в соответствии с пунктом 4.3 или пунктом 4.4 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Ответственность при организации парольной защиты

7.1. Ответственность за правильность формирования личных паролей пользователей возлагается на заведующего Учреждением.

7.2. Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

7.3. Ответственность за организацию парольной защиты в Учреждении возлагается на ответственного за информационную безопасность -заведующего Учреждением.

7.4. Пользователи за несоблюдение или нарушение парольной защиты несут ответственность в соответствии с действующим законодательством Российской Федерации.