Муниципальное бюджетное общеобразовательное учреждение «Обсерваторская средняя школа Зеленодольского муниципального района Республики Татарстан»

**ПРИНЯТО**
Педагогическим советом
(протокол №1 от 29.08.2023)

**УТВЕРЖДАЮ**
Директор МБОУ «Обсерваторская СОШ ЗМР РТ»

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ " ОБСЕРВАТОРСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА ЗЕЛЕНОДОЛЬСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЕСПУБЛИКИ ТАТАРСТАН"

Р.Р. Гимадиев

Введено в действие приказом №54/1-р
от 01.09.2022

**Инструкция пользователя информационной системыперсональных данных Муниципального бюджетного общеобразовательного учреждения «Обсерваторская средняя общеобразовательная школа Зеленодольского муниципального района Республики Татарстан»**

Настоящий документ подготовлен в рамках выполнения работ по обеспечению безопасной эксплуатации информационной системы персональных данных (далее - ИСПДн) Муниципального бюджетного общеобразовательного учреждения «Обсерваторская средняя общеобразовательная школа Зеленодольского муниципального района Республики Татарстан» (далее – Учреждение)

## 1. Общие положения.

1.1. Пользователь ИСПДн (далее - Пользователь) осуществляет обработку персональных данных в ИСПДн
1.2. Пользователем является каждый работник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
1.3. Пользователь несет персональную ответственность за свои действия.
1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, и другимирегламентирующими документами Учреждения.

## 2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования настоящей Инструкции и других внутренних распоряжений, регламентирующих порядок действий по защите персональных данных.

2.2. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других.

2.6. Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а также для получения консультаций по вопросам информационной безопасности необходимо обратиться к ответственному за организацию работы с ПД.

2.7. Пользователям запрещается:

− разглашать защищаемую информацию третьим лицам;

− копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

− самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

− несанкционированно открывать общий доступ к папкам на своей рабочей станции;

− отключать (блокировать) средства защиты информации;

− обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

− сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

− привлекать посторонних лиц для производства ремонта или настройки АРМ без согласования с ответственным за организацию работы с ПД.

2.8. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <CtrlxAlt><Del> и выбрать опцию <Блокировка>.

2.9. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределахвозложенных на него функций.

**3. Организация парольной защиты.**

3.1. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.2. Правила формирования пароля:

− пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

− пароль должен состоять не менее чем из 8 символов;

− в пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

− запрещается использовать в качестве пароля имя входа в систему,

простые пароли типа "123", "111", "qwerty" и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

– запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

– запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– запрещается выбирать пароли, которые уже использовались ранее.

3.3. Правила ввода пароля:

– ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

– во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамерами и др.).

3.4. Правила хранения пароля:

– запрещается записывать пароли на бумаге, в файле, в электронной записной книжке и на других носителях информации, в том числе на предметах;

– запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.5. Лица, использующие паролирование, обязаны:

– четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

– своевременно сообщать ответственным за организацию работы с ПД об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

**4. Правила работы в сетях общего доступа и (или) международного обмена**

4.1. Работа в сетях общего доступа и (или) международного обмена (сети "Интернет" и других) (далее - Сеть) на элементах ИСПДн должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

– осуществлять работу при отключенных средствах защиты (антивирусах и других);

– передавать по Сети защищаемую информацию без использования средств шифрования;

– посещать сайты сомнительной репутации (порносайты, сайты, содержащие нелегально распространяемое ПО, и другие).