

УТВЕРЖДАЮ

Директор МБОУ «Средняя  
общеобразовательная школа №31  
с углубленным изучением  
отдельных предметов» города  
Чебоксары Чувашской Республики  
\_\_\_\_\_Алексеев В.В.

Приказ № 0-36 от 01.02.2017г.

**Инструкция ответственного за обеспечение безопасности персональных данных  
в информационных системах персональных данных  
МБОУ "СОШ №31" г.Чебоксары**

**1. Общие положения**

1.1. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных МБОУ "СОШ №31" г. Чебоксары (далее – Ответственный) назначается приказом МБОУ "СОШ №31" г. Чебоксары (далее – Учреждение) и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн) Учреждения.

1.2. Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и защиты ПДн.

1.3. В своей деятельности Ответственный руководствуется Политикой в отношении обработки персональных данных в МБОУ "СОШ №31" г. Чебоксары, настоящей Инструкцией.

1.4. Методическое руководство работой Ответственного осуществляет ответственный за организацию обработки персональных данных (далее – Ответственный за организацию обработки ПДн).

**2. Обязанности ответственного за обеспечение безопасности персональных  
данных в информационных системах персональных данных**

Ответственный обязан:

2.1. Соблюдать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн при их обработке в ИСПДн.

2.2. Знать перечень обрабатываемых ПДн, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн.

2.3. Осуществлять общее техническое сопровождение ИСПДн:

– контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств;

– контролировать сохранность пломб на оборудовании автоматизированных рабочих мест;

– вести журнал учета и выдачи используемых материальных носителей ПДн;

– контролировать использование съемных материальных носителей информации;

– проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в ИСПДн Учреждения (далее – Пользователи ИСПДн) по правилам работы в ИСПДн.

2.4. Осуществлять настройку и сопровождение подсистемы регистрации и учета ИСПДн:

- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка сотрудников, допущенных к работе в ИСПДн;
- назначать пароли Пользователей ИСПДн;
- контролировать плановую смену паролей Пользователями ИСПДн для доступа в ИСПДн;
- своевременно удалять профиль Пользователя ИСПДн при увольнении или переводе сотрудника;
- вводить в базу данных системы защиты от несанкционированного доступа (далее – НСД) описания событий, подлежащих регистрации в системном журнале;
- регулярно проводить анализ системного журнала для выявления попыток несанкционированного доступа к ИСПДн;
- своевременно информировать ответственного за организацию обработки ПДн о несанкционированных действиях персонала для организации расследования попыток НСД.

2.5. Сопровождать подсистему обеспечения целостности рабочего программного обеспечения (ПО) ИСПДн:

- обеспечивать регулярное и своевременное обновление антивирусного программного обеспечения Учреждения;
- обеспечивать поддержание установленного порядка эксплуатации антивирусного программного обеспечения и соблюдение требований инструкции по антивирусной защите;
- обеспечивать регулярное и своевременное создание резервных копий ИСПДн Учреждения;
- осуществлять настройку и сопровождение системы защиты от НСД в ИСПДн.

2.6. Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИСПДн.

2.7. Требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

2.8. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и служебных расследований фактов НСД.

2.9. Участвовать при проведении внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн.

2.10. Контролировать выполнение Пользователями ИСПДн требований Инструкции пользователя информационных систем персональных данных МБОУ "СОШ №31" г. Чебоксары, а также установленных требований для обеспечения уровней защищенности ПДн.

2.11. Контролировать правильность применения Пользователями ИСПДн средств защиты информации.

2.12. В случае получения от Пользователей ИСПДн информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, незамедлительно принять все необходимые меры для обеспечения безопасности ПДн в пределах своих полномочий.

2.13. Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИСПДн:

- антивирусного программного обеспечения;
- средств защиты от несанкционированного доступа.

2.14. В случае нарушения работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.

2.15. Своевременно информировать Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ИСПДн.

### **3. Права ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных**

Ответственный имеет право:

3.1. Знакомиться с нормативными актами Учреждения, регламентирующими процессы обработки ПДн.

3.2. Требовать от Пользователей ИСПДн соблюдения требований Инструкции пользователя информационных систем персональных данных МБОУ "СОШ №31" г. Чебоксары и иных нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн.

3.3. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность ПДн, вносить свои предложения по совершенствованию организационных и технических мер защиты ПДн в ИСПДн.

3.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн.

3.5. Требовать прекращения работы в ИСПДн, как в целом, так и отдельных Пользователей ИСПДн, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИСПДн.

3.6. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.