



УТВЕРЖДАЮ
Директор
МОУ Чуфаровская СОШ
И. А. Медникова

» И.А. Медникова 2018

РЕГЛАМЕНТ
по управлению доступом к ресурсам информационной системы
«Автоматизированное рабочее место для подключения к защищенным
образовательным ресурсам» Муниципального общеобразовательного учреждения
Чуфаровской средней общеобразовательной школы

1. Общие положения

1.1. Настоящий регламент управления доступом к ресурсам информационной системы «Автоматизированное рабочее место для подключения к защищенным образовательным ресурсам» (далее – Информационная система) определяет порядок доступа субъектов доступа к объектам доступа в соответствии с законодательством Российской Федерации.

1.2. Регламент разработан в соответствии с:

- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Приказом ФСТЭК № 27 от 15 февраля 2017 г. «О внесении изменений в требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК от 11 февраля 2013 г.»;
- Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. В настоящем Регламенте используются следующие основные понятия:

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- государственная информационная система – федеральные и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов (п.1 ст. 13 149-ФЗ). Государственные информационные

системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях;

- защита персональных данных – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер обеспечения конфиденциальности информации о конкретном субъекте персональных данных.

2. Порядок доступа субъектов доступа к объектам доступа

2.1. Доступ к Информационной системе имеют допущенные сотрудники Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы. Доступ осуществляется с рабочих станций, установленных в здании Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы по адресу 433120, Ульяновская область, Вешкаймский район, р.п. Чуфарово, ул. Заводская, д. 11а (в пределах контролируемой зоны).

2.2. Субъектами доступа в Информационной системе являются:

- администратор Информационной системы – физическое лицо, сотрудник Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы, имеющий полный доступ к средствам вычислительной техники, настройкам программного обеспечения и базам данных Информационной системы. Все администраторы ознакомлены под роспись с инструкцией обеспечения безопасности Информационной системы;

- администратор информационной безопасности (ИБ) Информационной системы – физическое лицо, сотрудник Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы, имеющий полный доступ к средствам защиты информации и ответственный за обеспечение необходимого уровня безопасности. Все администраторы Информационной системы ознакомлены под роспись с инструкцией обеспечения безопасности Информационной системы;

- ответственный за защиту информации (ЗИ) – физическое лицо, сотрудник Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы, обладает полной информацией о конфигурации системы защиты Информационной системы (структура системы защиты, состав, места установки и параметров настройки средств защиты информации), обеспечивает руководство процессом обеспечения безопасности информации (лицом, ответственным за защиту информации считается лицо, ответственное за организацию обработки ПДн);

- пользователи – лица, сотрудники Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы, имеющие ограниченный удаленный доступ к элементам Информационной системы, необходимый им для отладки разработанных элементов системы и оперативного внесения изменений в систему. Все пользователи ознакомлены с данным

Регламентом. Физического доступа к серверным компонентам информационной системы, а также доступа к настройкам средств ее защиты пользователи не имеют.

2.3. Предоставление доступа пользователю к Информационной системе (или изменение прав доступа) осуществляется на основании Перечня лиц, уполномоченных на обработку персональных данных в Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы.

2.4. Назначение права доступа пользователя к персональным данным (далее – ПДн) в Информационной системе осуществляется в Информационной системе в соответствии с заявкой на предоставление пользователю права доступа к Информационной системе на имя руководителя организации. В случае принятия положительного решения о предоставлении пользователю доступа к Информационной системе информация о данном решении доводится до администратора Информационной системы, администратора ИБ Информационной системы, ответственного за ЗИ.

2.5. Все факты несанкционированного доступа и регистрации в Информационной системе, а также их последствия регистрируются с составлением администратором Информационной системы и администратором ИБ Информационной системы акта о несанкционированном доступе. В течение суток данный акт предоставляется ответственному за ЗИ.

2.6. Контроль за деятельностью пользователей Информационной системы осуществляется администратором ИБ и ответственным за ЗИ.

2.7. Категорически не допускается наличие у пользователей избыточных, неконтролируемых прав доступа, что является нарушением требований по обеспечению безопасности ПДн.

2.8. Основанием для прекращения права доступа пользователя к Информационной системе может служить его исключение из Перечня лиц, допущенных к обработке персональных данных лиц. Информация о данном решении доводится до администратора Информационной системы, администратора ИБ Информационной системы, ответственного за ЗИ.

2.9. Администратор ИБ обеспечивает выполнение требований по безопасности ПДн, обрабатываемых в Информационной системе в соответствии с классом Информационной системы и уровнем защищенности ПДн для подсистемы «Управление доступом субъектов доступа к объектам доступа», приведенным в приказе ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» с учётом изменений, изложенных в Приказе Федеральной службы по техническому и экспортному контролю № 27 от 15 февраля 2017 года «О внесении изменений в требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 №17»,; приказом ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных

данных при их обработке в информационных системах персональных данных».

2.10. На всех рабочих станциях должен быть установлен пароль на BIOS, соответствующий требованиям парольной политики. Все системные блоки рабочих станций, входящих в Информационную систему, должны быть опечатаны.

2.11. В Информационной системе предусмотрено:

автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования (90 дней);

автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования более 90 дней;

блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя (5 минут).

2.12. В Информационной системе после блокировки сеанса на устройстве отображения (мониторе) не должна отображаться информация сеанса пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы).

2.13. На автоматизированных рабочих местах Информационной системы запрещено устанавливать и использовать видеокamеры, микрофоны и другие регистрирующие устройства, а также выполнять несанкционированную удаленную активацию видеокamер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно.

2.14 В Информационной системе запрещено использование:

- технологий мобильного кода в любом виде;

- технологий передачи речи и/или видеосигнала в любом виде;

- технологий беспроводной передачи данных;

- неучтенных USB-накопителей информации. Реализация запрета осуществляется с помощью сертифицированного СЗИ «Secret Net Studio». Порядок использования данного СЗИ определен инструкцией пользователя и требованиями эксплуатационной документации (формуляра).

3. Ответственность за организацию управления доступом

3.1. Ответственность за организацию управления доступом субъектов доступа к объектам доступа в соответствии с требованиями настоящего Регламента возлагается на администратора ИБ.

3.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящего Регламента возлагается на ответственного за ЗИ.

3.3. Периодический контроль за выполнением всех требований настоящего Регламента осуществляется администраторами ИБ и ИС Муниципального общеобразовательного учреждения Чуфаровской средней общеобразовательной школы.

