

**ЕДИНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА УЧЕТА И
МОНИТОРИНГА ОБРАЗОВАТЕЛЬНЫХ ДОСТИЖЕНИЙ
ОБУЧАЮЩИХСЯ ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ
МОСКОВСКОЙ ОБЛАСТИ**

Регламент подключения типовых сегментов к Системе

2015

1 Общая часть

1.1 Назначение Регламента

Данный Регламент подключения типовых сегментов к Системе (далее – Регламент) предназначен для определения порядка подключения сегментов, соответствующих типовым, к Единой информационной системе учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области (далее – Система).

1.2 Основания для разработки и применения Регламента

Регламент разработан в соответствии с положениями, требованиями и рекомендациями следующих правовых и нормативных документов в области обеспечения информационной безопасности, действующих в Российской Федерации:

- Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;
- Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ;
- постановления Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119;
- приказа ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах персональных данных» от 11.02.2013 № 17;
- приказа ФСБ России «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10.07.2014 № 378;
- Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России 15.02.2008;

- «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России 14.02.2008;
- ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
- ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».

1.3 Область применения Регламента

Регламент применяется для определения порядка подключения сегментов, соответствующих типовым, к Системе.

1.4 Объекты регулирования Регламента

1.4.1 Субъекты и объекты взаимодействия

Субъектами взаимодействия являются следующие участники:

- педагогический и административный состав образовательных организаций, зарегистрированных в Системе;
- уполномоченные сотрудники муниципальных органов управления образованием и Министерства образования Московской области;
- технические специалисты образовательных организаций, зарегистрированных в Системе.

Объектом выступают сегменты соответствующие типовым. К таким сегментам Системы относятся следующие автоматизированные рабочие места (далее – АРМ):

- АРМ сотрудника Министерства образования;
- АРМ сотрудника муниципального органа управления образованием;
- АРМ сотрудника образовательной организации.

1.4.2 Термины и определения, обозначения и сокращения

АРМ	Автоматизированное рабочее место
Система	Единая информационная система учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области;
ГОСТ	Государственный стандарт;
НСД	Несанкционированный доступ;
ПДн	Персональные данные
ПО	Программное обеспечение;

ФЗ	Федеральный закон;
ФСБ	Федеральная служба безопасности;
ФСТЭК	Федеральная служба по техническому и экспортному контролю.

1.4.3 Права, обязанности и ответственность участников взаимодействия

Участники взаимодействия обязаны соблюдать требования, установленные следующими документами:

1. Политика в отношении обработки персональных данных.
2. Положение по организации и проведению работ по обеспечению безопасности информации при её обработке в Системе.
3. Положение об обработке ПДн.
4. Описание технологического процесса обработки информации.
5. Порядок обработки обращений субъектов персональных данных.
6. Положение об обработке ПДн.
7. Инструкция пользователя.

2 Порядок подключения

При подключении сегментов, соответствующих типовым, должны быть учтены следующие требования:

- требования по размещению технических средств;
- требования по установке общесистемного и специального ПО;
- требования по защите от несанкционированного доступа (далее – НСД) при эксплуатации АРМ;
- требования к защите от вредоносного кода.

На всех этапах подключения сегментов, соответствующих типовым, должна обеспечиваться защита информации от НСД. Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или администратором информационной безопасности. В организации, эксплуатирующей АРМ, должен быть назначен администратор информационной безопасности, на которого возлагаются задачи организации работ по использованию АРМ пользователя, выработки соответствующих инструкций для пользователей, а также контроль за соблюдением описанных ниже требований.

3 Технологические этапы подключения

Испытания сегментов, соответствующих типовым, проводятся в совокупности с серверной частью Системы с учетом особенностей технологического процесса обработки информации в Системе, в том числе – взаимодействия сегмента с серверной частью Системы. Требования к сегменту учитывают необходимость соответствия классов защищенности, угроз безопасности информации и проектных решений по информационной системе в подключаемых сегментах, определенным для типового. Испытания проводятся в соответствии с требованиями Приказа ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах персональных данных» от 11.02.2013 № 17. По результатам испытаний оформляются протоколы испытаний, акт соответствия сегмента Системы требованиям по защите информации. После окончания работ подать заявку, включающую в качестве приложения копию Акта соответствия, в Министерство образования Московской области на выпуск акта распространения действия аттестата Системы. Комиссия, сформированная Министерством образования Московской области, проводит проверку соблюдения требований аттестата. Если требования соблюдены, то организации выдается акт распространения действия аттестата Системы и копия аттестата Системы

4 Требования к типовым сегментам Системы

Требования к типовым сегментам Системы изложены в документе «Единая информационная система учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области. Требования к типовому сегменту Системы», в разделе 2.

5 Условия изменения и прекращения действия Регламента

5.1 Период

Настоящий Регламент и его изменения считаются действующими с момента публикации до момента прекращения его действия.

5.2 Прекращение

Настоящий Регламент периодически исправляется и дополняется, оставаясь действующим до публикации новой версии, уведомления о прекращении его действия.