Разъяснения по безопасности для муниципальных органов управления образованием и общеобразовательных организаций Московской области

25 августа 2015 г. была завершена аттестация Единой информационной системы учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области (далее – Система, ГИС ИСУОД).

В соответствии с требованиями п.8 Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах персональных данных». Система аттестована в составе: серверная часть Системы и три типовых сегмента. Типовые сегменты это:

- общеобразовательная организация в Московской области;
- муниципальный орган управления образованием Московской области;
- Министерство образования Московской области.

При проведении аттестации Системы использованы нормы, требования и рекомендации, приведенные в следующих нормативных правовых и иных актах:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства РФ № 687 от 15.09.2008 г. «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Приказ Государственной технической комиссии при президенте Российской Федерации от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)».
- Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
- Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах персональных данных».

– Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава 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».

Главная задача подготовки муниципальных органов управления образованием Московской области и общеобразовательных организаций в Московской области (далее – организации) к распространению действия аттестата на Систему – это приведение в соответствие требованиям законодательства по защите персональных данных (далее – ПДн) рабочих мест сотрудников. Рекомендуется начать с рабочего места администратора Системы в организации, так как сотрудник организации с этой ролью имеет максимально возможное количество прав и привилегий в Системе, а также доступ ко всем ПДн в Системе. Для корректной работы и обеспечения информационной безопасности в организации необходимо защитить все рабочие места сотрудников, или организационными методами ограничить возможность работы в Системе сотрудников только с защищенного рабочего места.

Для оптимизации работ по приведению системы безопасности в организации в соответствие требованиям законодательства в приложении к данному разъяснению приведены следующие документы:

1. Требования к типовым сегментам Системы.
2. Регламент подключения типовых сегментов к Системе.
3. Пакет шаблонов организационно-распорядительных документов.
4. Проект акта соответствия сегмента информационной системы «Единая информационная система учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области» условиям распространения аттестата соответствия №1033.

Для обеспечения безопасности Системы и соответствия требованиям законодательства у руководителя организации есть два варианта действий:

1) Организовать систему информационной безопасности в организации в соответствии с требованиями к типовым сегментам и получить акт распространения аттестата соответствия на сегмент ГИС ИСУОД, расположенный в организации (далее – Сегмент).

2) Организовать систему информационной безопасности и провести аттестационные испытания собственной Муниципальной информационной системы (далее – МИС). Аттестовать необходимо рабочее место администратора Системы с учетом его информационного взаимодействия с серверной частью ГИС ИСУОД, размещенной в Центре обработке данных Правительства Московской области (далее – ЦОД). В целях обеспечения

информационного взаимодействия МИС с серверной частью ГИС ИСУОД, проведение аттестационных испытаний предварительно необходимо согласовать с Министерством образования Московской области.

Если организация приняла решение соответствовать требованиям типового сегмента, необходимо:

1. Произвести закупку, установку и настройку недостающих средств защиты информации в Сегменте.

Для выполнения требований, предъявляемых к типовому сегменту, в организации необходимо наличие следующих СЗИ (приведен список СЗИ на одно рабочее место):

- Secret Net 7. Производитель ООО «Код Безопасности». Сертификат ФСТЭК №2707 от 07.09.2012 г.
- Security Studio Endpoint Protection. Производитель ООО «Код Безопасности»; Сертификат ФСТЭК №3128 от 17.04.2014 г.
- VipNet Client КС3. Производитель ОАО «ИнфоТеКС». Сертификат соответствия ФСБ России № СФ/525-2224. (При покупке следует указать необходимость лицензии для включения в сеть № 2131).

2. Разработать и утвердить пакет организационно-распорядительных документов Сегмента.

Список Организационно-распорядительной документации, необходимой для выполнения требований к типовому сегменту Системы:

№ п/п	Наименование документа
1.	Политика в отношении обработки персональных данных.
2.	Приказ «Об организации работ по защите персональных данных при их обработке в государственной информационной системе»
3.	Приказ о назначении администратора информационной безопасности
4.	Перечень сотрудников, допущенных к обработке ПДн
5.	Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных
6.	Положение о порядке организации и проведения работ по обеспечению безопасности информации при её обработке в Системе
7.	Перечень сведений конфиденциального характера организации
8.	Положение о разрешительной системе доступа работников к защищаемым информационным ресурсам ГИС ИСОУД
9.	Перечень защищаемых информационных ресурсов ГИС ИСОУД
10.	Инструкция администратора информационной безопасности
11.	Инструкция пользователя
12.	Инструкция по организации парольной защиты в Сегменте ГИС ИСОУД
13.	Инструкция по антивирусной безопасности
14.	Положение об обработке персональных данных.
15.	Инструкция по архивации информационных ресурсов Системы
16.	Порядок обработки обращений субъектов персональных данных

№ п/п	Наименование документа
17.	Журнал учета съемных носителей информации, содержащих персональные данные
18.	Журнала учета средств защиты информации
19.	Инструкция по обработке персональных данных без использования средств автоматизации
20.	Журнал учета мероприятий по контролю обеспечения защиты персональных данных
21.	Журнал учета инцидентов информационной безопасности

3. Провести приемочные испытания Сегмента. В ходе приемочных испытаний необходимо провести процедуру подтверждения соответствия Сегмента условиям распространения аттестата соответствия № 1033 с оформлением Акта соответствия.

4. После окончания работ подать заявку, включающую в качестве приложения копию Акта соответствия, в Министерство образования Московской области на выпуск акта распространения действия аттестата Системы.

5. 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.

6. В случае проверки регуляторами в организации до получения аттестата, предъявить собственный утвержденный руководителем организации план мероприятий по приведению системы информационной безопасности в соответствие требованиям нормативных документов.

Мероприятия по закупке, установке и настройке СЗИ должны проводится с привлечением на договорной основе организации, имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Мероприятия 2 – 3 могут проводиться силами организации, эксплуатирующей Сегмент, при наличии в штате организации специалистов в области защиты информации, либо с привлечением на договорной основе организации, имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации. При необходимости привлечения для выполнения работ сторонней организации выбор организации осуществляет организация, эксплуатирующая Сегмент.

Если организация приняла решение организовать систему информационной безопасности и провести аттестационные испытания МИС, необходимо:

1. Самостоятельно найти и подписать договор с любой аттестующей организацией, имеющей лицензию ФСТЭК «На деятельность по технической защите конфиденциальной информации».

2. Произвести закупку, установку и настройку средств защиты информации.

3. Разработать пакет нормативных документов. Требования к пакету ОРД будут предъявлены аттестующей организацией в процессе аттестации.

4. Провести аттестационные испытания МИС. Аттестационные испытания МИС должны проводиться с учетом ее взаимодействия с серверной частью ГИС ИСУОД, расположенной в ЦОД. Для обеспечения информационного взаимодействия МИС с серверной частью ГИС ИСУОД необходимо согласовать проведение работ с Министерством образования Московской области.

5. Получить аттестат на собственную МИС.

6. В случае проверки регуляторами в организации до получения аттестата, предъявить собственный утвержденный руководителем организации план мероприятий по приведению системы информационной безопасности в соответствие требованиям нормативных документов.

Приложения:

1. Требования к типовым сегментам Системы на 8 л. в 1 экз.
2. Регламент подключения типовых сегментов к Системе на 5 л. в 1 экз.
3. Пакет шаблонов организационно-распорядительных документов на 48 л. в 1 экз.
4. Форма акта соответствия сегмента информационной системы «Единая информационная система учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области» условиям распространения аттестата соответствия №1033 на 2 л. в 1 экз.
5. Образцы согласий на обработку персональных данных на 11 л. в 1 экз.