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

Требования к типовым сегментам Системы

Введение

Данный документ содержит перечень требований по обеспечению информационной безопасности автоматизированных рабочих мест пользователей единой информационной системы учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области (далее – Системы).

Меры по обеспечению информационной безопасности сегментов Системы должны определяться Политикой информационной безопасности, разработанной в соответствии с требованиями:

- Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Заместителем директора ФСТЭК России от 15.02.2008 г.;
- 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 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» от 10.07.2014 № 378.

1 Типовые сегменты Системы

1.1 Полное наименование системы, обозначение

Полное наименование Системы: «Единая информационная система учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области».

Краткое наименование Системы: «ИСУОД».

Далее по тексту также используется сокращенное условное обозначение и «Система».

1.2 Виды типовых сегментов Системы

К типовым сегментам Системы относятся следующие автоматизированные рабочие места (далее – АРМ):

– АРМ сотрудника Министерства образования;

– АРМ сотрудника муниципального органа управления образованием;

– АРМ сотрудника образовательной организации.

Все АРМ, являющиеся типовыми сегментами Системы, взаимодействуют с Системой посредством прямого подключения к сети Интернет.

Требования, предъявляемые к АРМ сотрудника образовательной организации, АРМ сотрудника Министерства образования и АРМ сотрудника муниципального органа управления образованием, идентичны друг другу (в документе все АРМ условно названы «АРМ пользователя»).

АРМ сотрудника образовательной организации, АРМ сотрудника Министерства образования и АРМ сотрудника муниципального органа управления образованием являются элементами информационной системы персональных данных (далее – ГИС), на которую распространяется система защиты персональных данных (далее – СЗПДн), разработанная в соответствии с Политикой информационной безопасности Системы.

2 Требования по организации работ по защите от НСД

Защита информации от несанкционированного доступа (далее – НСД) должна обеспечиваться на всех технологических этапах обработки информации, в том числе при проведении ремонтных и регламентных работ. 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.

2.1 Требования по размещению технических средств

При размещении технических средств с установленным АРМ пользователей:

- должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным АРМ пользователя, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им персональных и статистических данных.

2.2 Требования по установке общесистемного и специального ПО

К установке общесистемного и специального программного обеспечения (далее – ПО) допускаются лица, изучившие документацию на ПО. При установке ПО на АРМ пользователя необходимо соблюдать следующие требования:

1. На технических средствах, предназначенных для работы с АРМ пользователя, использовать только лицензионное ПО фирм-изготовителей.

2. Установку ПО АРМ пользователей необходимо производить только с зарегистрированного, защищенного от записи носителя.

3. На АРМ пользователя не должны устанавливаться средства разработки ПО и отладчики.

4. Предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части технических средств, на которых установлено ПО АРМ пользователя (например, путем опечатывания системного блока и разъемов АРМ пользователя).

5. После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО на АРМ пользователей.

6. ПО, устанавливаемое на АРМ пользователей, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;

- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

2.3 Требования по защите от НСД при эксплуатации АРМ

Для обеспечения защиты от НСД при эксплуатации АРМ пользователя необходимо учитывать следующие требования:

1. Должна быть предусмотрена система подтверждения легитимности пользователя при просмотре данных, включающая два этапа:
   - аутентификацию – сопоставление предъявленных пользователем уникального идентификатора (логина) и соответствующего ему пароля с учетными записями зарегистрированных пользователей, хранящимися в информационной базе Системы;
   - авторизацию – сравнение набора прав, присвоенных учетной записи аутентифицированного пользователя с требуемыми для доступа к запрошенному ресурсу, функции, интерфейсу, информационному объекту.
2. Для всех пользователей должна быть запрещена возможность удаления преднастроенных объектов и отчетности.
3. Выполнение привилегированных операций (редактирование, удаление данных и др.) должно сопровождаться механизмом двойного подтверждения выполнения со стороны пользователя.
4. Должен быть предусмотрен механизм смены пароля для пользователей, при смене пароля в обязательном порядке должно запрашиваться его предыдущее значение.
5. При использовании механизма отсылки по электронной почте забытого пароля должна осуществляться проверка на соответствие учетной записи и электронного адреса.
6. Должен осуществляться контроль непротиворечивости и форматного соответствия вводимых данных.
7. Для снижения ошибочных действий пользователей должно быть разработано полное и доступное руководство пользователя.
8. Интерфейс должен быть реализован с учетом свойственных для пользователя задач (функциональная группировка пунктов меню или их аналогов в соответствии с функциями, задачами и технологией работы пользователя).

Для обеспечения защиты передаваемых с АРМ данных в Системе должны быть предусмотрены следующие методы:

- осуществление контроля получаемой информации на отсутствие вредоносного программного кода и управляющих последовательностей;
- осуществление защиты каналов связи.

В случае если пользователем АРМ не предъявлен логин и пароль, или они не соответствуют ни одной учетной записи, пользователь будет рассматриваться как анонимный. Анонимный пользователь будет аутентифицироваться специальной системной учетной записью с фиксированным набором прав, позволяющим реализовать открытый доступ к определенным ресурсам.

Программное обеспечение Системы не должно допускать возможности использования косвенного доступа к объектам и данным. Не должна предоставляться возможность получения содержимого закрытого информационного объекта путем вызова открытых функций Системы с указанием адреса закрытого источника.

В случае обнаружения несанкционированного вмешательства в данные Системы пользователь АРМ должен обращаться в службу поддержки пользователей системы или непосредственно к администратору Системы: описать признаки и предполагаемый характер вмешательства, указать перечень данных, подвергшихся вмешательству.

В качестве существующих технических решений в ГИС применяется программный продукт Secret Net 7. Производитель ООО «Код Безопасности». Сертификат ФСТЭК №2707 от 07.09.2012 г.

2.4 Требования к защите от вредоносного кода

Вредоносный код – любой программный код (компьютерный вирус, троян, сетевой червь), приводящий к нарушению функционирования средств вычислительной техники и/или предназначенный для искажения, модификации, уничтожения, блокирования или несанкционированного копирования информации.

Возможен следующий характер проявлений действий вредоносного кода (далее – ВК):

- искажение изображения на экране монитора;
- искажение символов, вводимых с клавиатуры;
- блокирование клавиатуры, звуковые эффекты;
- стирание или порча отдельных частей диска или файлов;
- повреждение загрузочных секторов жесткого диска ПЭВМ;

- остановка загрузки или зависание компьютера, значительное замедление его работы;
- уничтожение или искажение информации о системной конфигурации АРМ пользователя.

ВК может попасть на компьютер со сменного носителя (CD-ROM, USB флеш-накопителей и других носителей, даже если эти носители не содержат файлов), при загрузке файлов из сети, с сообщением, полученным по электронной почте, а также через уязвимости операционных систем просто при наличии сетевого подключения компьютера к локальной вычислительной сети. При наличии технической возможности, обновление средств защиты и сигнатурных баз должно производится централизованно, с рабочего места администратора программных средств.

В целях обеспечения защиты от воздействий вредоносного кода пользователю АРМ запрещается:

- самостоятельно устанавливать программное обеспечение, в том числе командные файлы;
- использовать при работе «зараженный» вредоносным кодом либо с подозрением на «заражение» носитель и/или файл;
- использовать личные носители на АРМ пользователя;
- самостоятельно проводить “лечение” носителя и/или файла;
- самостоятельно отключать, удалять и изменять настройки установленных средств защиты.

Пользователь АРМ обязан:

- проводить контроль на отсутствие ВК любых сменных и подключаемых носителей (CD-дисков, DVD-дисков, USB флеш-накопителей и т.п.) и файлов;
- входной контроль на отсутствие ВК компакт-дисков и DVD-дисков, предназначенных для одноразовой записи информации, проводит получатель (владелец) диска однократно с момента приобретения (получения) диска перед использованием его на компьютерах;
- обращаться в службу поддержки пользователей системы или непосредственно к администратору Системы.

В качестве существующих технических решений в ГИС применяется программный продукт Security Studio Endpoint Protection. Производитель ООО «Код Безопасности»; Сертификат ФСТЭК №3128 от 17.04.2014 г.

2.5 Требования по криптографической защите информации

В соответствии с требованиями приказа ФСБ 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», а также документов «Модель вероятного нарушителя» и «Модель угроз безопасности информации», исходя из уровня защищенности персональных данных и актуальных угроз безопасности персональных данных необходимо использовать СКЗИ класса КС1 и выше.

В качестве существующих технических решений в ГИС применяется программный продукт «VIPNet Client 3.2», соответствующий требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3, что подтверждается сертификатом соответствия № СФ/525-2224.

3 Список сокращений и обозначений

АРМ	Автоматизированное рабочее место.
ВК	Вредоносный код.
ГИС	Государственная информационная система.
ИСУОД	Аппаратно-программный единой информационной системы учета и мониторинга образовательных достижений обучающихся общеобразовательных организаций Московской области.
НСД	Несанкционированный доступ.
ПО	Программное обеспечение.
ПЭВМ	Персональная электронная вычислительная машина.
СЗПДн	Система защиты персональных данных.
СКЗИ	Средства криптографической защиты информации
ФСБ	Федеральная служба безопасности.
ФСТЭК	Федеральная служба по техническому и экспортному контролю.