ТРЕБОВАНИЯ ДЛЯ РАСПРОСТРАНЕНИЯ АТТЕСТАТА СООТВЕТСТВИЯ РЕГИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ РОСТОВСКОЙ ОБЛАСТИ «ОБРАЗОВАНИЕ» ПОЛЬЗОВАТЕЛЬСКИЙ СЕГМЕНТ НА ДРУГИЕ СЕГМЕНТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ

1 ВВЕДЕНИЕ

Данный документ содержит перечень требований к типовым автоматизированным рабочим местам (далее - ТАРМ) региональной информационной системы Ростовской области «Образование» пользовательский сегмент (далее – РИСО).

Выполнение данных требований обязательно для распространения аттестата соответствия РИСО требованиям по безопасности информации (№ АСп0462, выдан 23.08.2019 г.) на ТАРМ.

Сегмент с ТАРМ считается соответствующим ранее аттестованному сегменту РИСО если для указанных сегментов установлены одинаковые классы защищенности, угрозы безопасности информации, реализованы одинаковые проектные решения по информационной системе и ее системе защиты информации.

Требования разработаны в соответствии со следующими нормативно-правовыми актами:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федерального закона от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.).

- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- Приказ ФСБ России от 10 июля 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».
- Приказ 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».
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
- Методический документ «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК 11 февраля 2014 г.
- Руководящий документ Гостехкомиссии России «Средства

вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

2 ТРЕБОВАНИЯ К ОРГАНИЗАЦИОННОМУ ОБЕСПЕЧЕНИЮ

Порядок предоставления доступа к РИСО указан в «Положение о региональной информационной системе Ростовской области «Образование»» утвержденным постановлением министерства общего и профессионального образования Ростовской области от 12.11.2018 № 8. Ознакомиться с положением можно по адресу в сети интернет: http://support.ris61edu.ru/razdel-ris_obrazovanie/.

В юридическом лице, для получения доступа к РИСО, необходимо назначить сотрудника, ответственного за обеспечение безопасности информации. В рамках своих обязанностей данный сотрудник должен:

- осуществлять обработку конфиденциальной информации, не относящейся к государственной тайне, с ТАРМ;
- ознакомиться под роспись и выполнять требования организационно-распорядительной документации на аттестованную РИСО;
- выполнять инструкцию пользователя ТАРМ;
- осуществлять контроль над выполнением требований, перечисленных в пункте 3 настоящего документа;
- оповещать администратора безопасности РИСО о любых инцидентах информационной безопасности;
- в случае нарушения и/или невозможности выполнять вышеизложенные требования немедленно прекратить обработку конфиденциальной информации.

Для ТАРМ должны быть актуальны такие же угрозы безопасности информации, как и в аттестованной части РИСО. Если в ТАРМ выявлены новые угрозы безопасности информации, распространения аттестата соответствия РИСО невозможно.

На ТАРМ до начала установки СЗИ необходимо произвести анализ уязвимостей информационной системы и принятие мер по их устранению.

Данные о ТАРМ нужно указывать в техническом паспорте на РИСО. В техническом паспорте обязательно указываются следующие данные:

- наименование системы;
- расположение системы;
- класс системы;
- перечень основных технических средств и систем, входящих в состав системы;
- структура, топология и размещение основных технических средств и систем относительно границ контролируемой зоны объекта;
- перечень средств защиты информации, установленных в системе;
- перечень используемых в системе программных средств.

3 ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИИ РАБОТ ПО ЗАЩИТЕ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

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 ТАРМ или администратором информационной безопасности РИСО.

3.1 ТРЕБОВАНИЯ ПО РАЗМЕЩЕНИЮ ТЕХНИЧЕСКИХ СРЕДСТВ

При размещении технических средств с установленным ТАРМ:

- должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным ТАРМ, 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.

3.2 ТРЕБОВАНИЯ ПО УСТАНОВКЕ ОБЩЕСИСТЕМНОГО И СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Требование обязательного использования лицензионного программного обеспечения содержится в условиях использования сертифицированных средств защиты информации. Для общесистемного и специального ПО должны быть документы, подтверждающие легальность использования данного ПО.

На рабочем месте должна быть установлена одна из редакций операционной системы:

- Windows 10 (32/64-разрядная);
- Windows 8.1 (32/64-разрядная);
- Windows 7 SP1 (32/64-разрядная).

После получения заключения о присоединении ТАРМ к аттестованной РИСО, запрещается установка, удаление, модификация и иные действия с программным обеспечением ТАРМ любым лицом, кроме администратора РИСО.

4 ТРЕБОВАНИЯ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

4.1 ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (НСД)

Для ОС семейства «Windows» защита от несанкционированного доступа должна быть обеспечена применением сертифицированного средства защиты от несанкционированного доступа (СЗИ от НСД) 6 класса, не ниже 5 класса защищенности по СВТ.

СЗИ от НСД должно выполнять следующие функции:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- регистрация событий безопасности;
- обеспечение целостности информационной системы и информации.

Установка и настройка СЗИ от НСД производится на ТАРМ в соответствии с эксплуатационной документацией производителя.

4.2 ТРЕБОВАНИЯ К АНТИВИРУСНОЙ ЗАЩИТЕ

Антивирусная защита создается для обеспечения безопасности защищаемой информации и программно-аппаратной среды РИСО, обеспечивающей обработку этой информации, выявления и предотвращения вирусного воздействия.

Антивирусная защита должна быть обеспечена применением сертифицированного средства антивирусной защиты САВЗ типа «В» не ниже 4 класса защиты.

При функционировании РИСО предусмотрено использование съемных носителей информации. В этом случае должны использоваться средства антивирусной защиты для их проверки.

Приложение проверяет все запускаемые, открываемые и модифицируемые файлы, проводит лечение или удаление зараженных объектов, а также изолирует подозрительные объекты в карантинном хранилище для дальнейшего анализа. Приложение также проводит антивирусную проверку заданных областей по запросу администратора или по расписанию.

Обновление антивирусных баз и выполнение периодических проверок осуществляется в соответствии с эксплуатационной документацией.

Установка и настройка компонентов антивируса на ТАРМ должна осуществляться с сертифицированного дистрибутива в соответствии с эксплуатационной документацией производителя.

4.3 ТРЕБОВАНИЯ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ И МЕЖСЕТЕВОМУ ЭКРАНИРОВАНИЮ

В качестве подсистемы межсетевого экранирования и криптографической защиты информации требуется использование программных комплексов линейки ViPNet от производителя ОАО «Инфотекс».

Защищенное подключение к РИСО возможно следующими СЗИ:

- ПО ViPNet client 4.x.

4.3.1 ПО VIPNET CLIENT

Для ОС семейства «Windows» на рабочем месте пользователя должен быть установлен программный комплекс, выполняющий на рабочем месте пользователя или сервере с прикладным ПО функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования ViPNet client версии 4. Сертификат соответствия ФСБ России № СФ/515-3772 от 25.10.2019 на соответствие изделия «Программный комплекс ViPNet Client 4» требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности.

Установка и настройка компонентов межсетевого экранирования и криптографической защиты информации на ТАРМ должна осуществляться в соответствии с эксплуатационной документацией производителя.

Подключение ViPNet Client должно осуществляться к защищенной сети № 5203.

5 РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ

В случае выполнения вышеизложенных требований ТАРМ могут пройти аттестационные испытания в соответствии с программой и методикой проведения аттестационных испытаний РИСО.

В аттестационную документацию вносятся данные о заключении по результатам аттестационных испытаний на соответствие требований по информационной безопасности.

6 ЕДИНЫЙ ГЛОССАРИЙ СОКРАЩЕНИЙ

Сокращение	Определение
РИСО	Региональная информационная система Ростовской области «Образование» пользовательский сегмент
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
САВЗ	Средства антивирусной защиты
МЭ	Межсетевой экран
СЗИ	Средство защиты информации
ТАРМ	Типовое автоматизированное рабочее место
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ФСБ	Федеральная служба безопасности