МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 23

Подписано цифровой подписью: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 23
Дата: 2023.02.27 14:52:50 +04'00'

Приложение № 2
к приказу МБОУ СОШ № 23
от 15.06.2021 № 209-ОД

ИНСТРУКЦИЯ

по обеспечению информационной безопасности типовых автоматизированных рабочих мест пользователей (далее - ТАРМ) регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам в Ростовской области (далее – РИС) в МБОУ СОШ № 23

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция (далее – "Инструкция") разработана для установления единого перечня требований по обеспечению информационной безопасности ТАРМ РИС.

1.2. При разработке Инструкции использовались следующие нормативные акты Российской Федерации:

- 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..
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена ФСТЭК 15.02.2008 г.
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена ФСТЭК 15 февраля 2008 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

В школе приказом директора назначается сотрудник, ответственный 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 РИС;
- выполнять инструкцию пользователя ТАРМ;
- осуществлять контроль над выполнением требований по защите от несанкционированного доступа;
- оповещать администратора безопасности РИС о любых инцидентах информационной безопасности;
- в случае нарушения и/или невозможности выполнять вышеизложенные требования немедленно прекратить обработку конфиденциальной информации.

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 РИС.

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

После получения акта присоединения ТАРМ к аттестованной РИС, запрещается установка, удаление, модификация и иные действия с программным обеспечением ТАРМ любым лицом, кроме администратора РИС.

4. ТРЕБОВАНИЯ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

4.1 ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (НСД)

Защита от несанкционированного доступа должна быть обеспечена применением сертифицированного средства защиты от несанкционированного доступа (СЗИ от НСД) – Secret Net 7. Производитель ООО «Код Безопасности». Сертификат ФСТЭК №2707 от 07.09.2012 г.

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 РИС, обеспечивающей обработку этой информации, выявления и предотвращения вирусного воздействия.

Антивирусная защита должна быть обеспечена одним из сертифицированных средств антивирусной защиты:
- «Kaspersky Endpoint Security 10». Производитель ЗАО «Лаборатория Касперского». Сертификат ФСТЭК № 3025 от 26.07.2012 г.;
- «ESET NOD32 Secure Enterprise Pack (версия 5.0)». Производитель ООО «ИСС Дистрибьюшн». Сертификат ФСТЭК № 3243 от 13.10.2014 г.;
- «Dr.Web Enterprise Security Suite». Производитель ООО «Доктор Веб». Сертификат ФСТЭК № 3509 от 27.01.2016 г.

При функционировании РИС 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.

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 (Производитель ОАО «ИнфоТеКС) одной из следующих версий:

- версия 3.2. Сертификат соответствия ФСБ России № СФ/525-2224 от 25.09.2013 г.;
- версия 4. Сертификат соответствия ФСБ России № СФ/515-2907 от 17.06.2016 г., Сертификат соответствия ФСБ России № СФ/124-2876 от 30.03.2016 г.

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. ViPNet Client (Клиент) состоит из набора взаимосвязанных программных модулей:

- ViPNet [Монитор].
- ViPNet [Контроль приложений].
- ViPNet [Деловая Почта].
- ViPNet MFTP.
- Криптопровайдер ViPNet CSP.

ViPNet [Монитор] — совместно с низкоуровневым драйвером шифрования и фильтрации трафика отвечает за реализацию функций:

- персонального сетевого экрана — надежно защищает рабочую станцию/сервер от возможных сетевых атак, как из глобальной (Интернет), так и из локальной сети;
- шифратора IP-трафика — обеспечивает защиту (конфиденциальность, подлинность и целостность) любого вида трафика (приложений, систем управления и служебного трафика ОС), передаваемого между любыми объектами защищенной сети, будь то рабочие станции, файловые серверы, серверы приложений. Высокая производительность шифрующего драйвера, поддерживающего современные многоядерные процессоры, позволяет в реальном времени защищать трафик служб голосовой и видеосвязи в сетях TCP/IP и обеспечивать одновременную работу множества пользовательских сессий. Поддерживается прозрачная работа через устройства статической и динамической NAT/PAT маршрутизации при любых способах подключения к сети;
- чат-клиента — позволяет пользоваться услугами встроенного сервиса обмена защищенными сообщениями и организации чат-конференций между объектами защищенной сети ViPNet, на которых установлены ViPNet Client или ViPNet Coordinator (Windows);

- клиента службы обмена файлами — позволяет обмениваться между объектами защищенной сети ViPNet любыми файлами без установки дополнительного ПО (например, FTP-сервера/клиента) или использования функций ОС по общему доступу к файлам через сеть. Обмен файлами производится через защищенную транспортную сеть ViPNet с гарантированной доставкой и «докачкой» файлов при обрыве связи.

ViPNet [Контроль приложений] — программа, которая позволяет контролировать сетевую активность приложений и компонент операционной системы.

При этом можно формировать «черный» и «белый» списки приложений, которым запрещено или разрешено работать в сети, а также задавать реакцию на сетевую активность неизвестных приложений.

В большинстве случаев это позволяет предотвратить несанкционированную сетевую активность вредоносного ПО, например, программ-«троянов».

ViPNet [Деловая Почта] — программа, которая выполняет функции почтового клиента защищенной почтовой службы, функционирующей в рамках защищенной сети ViPNet. Любой отправитель корреспонденции может быть однозначно идентифицирован. Поэтому этот сервис ViPNet является идеальным решением для внутрикорпоративного обмена документами и письмами.

ViPNet MFTP – программа, выполняющая функции обмена служебной информацией между узлами защищенной сети (обновления ключей шифрования, связей узлов, программного обеспечения) и конвертами с письмами «Деловой Почты» и конвертами «Файлового Обмена».

Криптопровайдер ViPNet CSP – встроенный в ViPNet Client криптопровайдер, реализующий стандартный для разработчиков прикладных систем под ОС Windows интерфейс Microsoft CryptoAPI 2.0.