ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ КУРГАНСКОЙ ОБЛАСТИ

ПРИКАЗ

от 16.01.2018 № 31

г. Курган

Об утверждении требований информационной безопасности рабочих мест в Департаменте образования и науки Курганской области

В соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» ПРИКАЗЫВАЮ:

1. Утвердить требования по обеспечению информационной безопасности автоматизированных рабочих мест пользователей при работе с информационными системами Департамента образования и науки Курганской области (приложение).

2. Контроль за исполнением настоящего приказа возложить на первого заместителя директора Департамента образования и науки Курганской области Кочерова А.Б.

Директор Департамента образования и науки
Курганской области Н.Д. Бобкова

Моторин Г.П.
8(3522)462829

УТВЕРЖДЕНЫ

приказом директора Департамента образования и науки Курганской области

от 16.01.2018 № 31

Требования по обеспечению информационной безопасности автоматизированных рабочих мест пользователей при работе с информационными системами Департамента образования и науки Курганской области

город Курган, 2017 год

Оглавление

1 Введение 3
2 Общие положения 4
3 Требования к организационному обеспечению 4
4 Требования по организации работ по защите от несанкционированного доступа 5
4.1 Требования по размещению технических средств 5
4.2 Требования по установке общесистемного и специального программного обеспечения 5
4.3 Требования к разработке системы защиты информации для сегмента информационной системы 5
5 Требования по технической защите информации 6
5.1 Требования по организации защиты АРМ от несанкционированного доступа 6
5.2 Требования к антивирусной защите 7
5.3 Требования по криптографической защите информации и межсетевому экранированию 7
5.4 Требования к анализу защищенности 8

1 ВВЕДЕНИЕ

Данный документ содержит перечень требований по обеспечению информационной безопасности автоматизированных рабочих мест пользователей (далее - АРМ) при работе с информационными системами (далее – ИС) Департамента образования и науки Курганской области (далее - Департамент).

Выполнение данных требований является обязательным для организаций, планирующих осуществлять подключение к информационным системам Департамента (далее-претендент).

Требования разработаны в соответствии со следующими нормативными правовыми актами:

– Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1].

– Федеральный закон от 04 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности» [2].

– Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [3].

– Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.) [4].

– Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [5].

– Приказ ФСБ России от 10 июля 2014 года № 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» [6].

– Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [7].

– Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [8].

– Методический документ «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК 11 февраля 2014 года [9].

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена ФСТЭК 15 февраля 2008 года) [10].

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена ФСТЭК 15 февраля 2008 года) [11].

– Информационное сообщение ФСТЭК России от 28 апреля 2016 года № 240/24/1986 «Об утверждении требований к межсетевым экранам» [12].

– ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения [13].

2 ОБЩИЕ ПОЛОЖЕНИЯ

В ИС Департамента ведется обработка персональных данных, таким образом к ним применяются требования к информационным системам персональных данных (далее - ИСПДн).

Согласно ст.2 документа [1] оператор информационной системы - гражданин или юридическое лицо, осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базе данных. Таким образом, оператором ИС является как Департамент, так и Учреждения, эксплуатирующие ИС Департамента.

Организация, осуществившая подключение к ИС Департамента, является оператором сегмента ИС Департамента и согласно ст.16 ч.4 документа [1] обязана обеспечить:

1. Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2. Своевременное обнаружение фактов несанкционированного доступа к информации;
3. Предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4. Недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5. Возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6. Постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, организация-претендент обязана реализовать вышеуказанные требования и дополнительно:

– закупить необходимые средства защиты информации в соответствии с техническими решениями рекомендуемыми настоящим документом, установить и настроить их;

– провести процедуру аттестации АРМ пользователя сегмента ИС по требованиям безопасности информации.

3 ТРЕБОВАНИЯ К ОРГАНИЗАЦИОННОМУ ОБЕСПЕЧЕНИЮ

Организация-претендент при подключении к ИС Департамента должна выполнить следующие организационные меры:

– назначить сотрудника, ответственного за обеспечение безопасности информации в сегменте ИС. В рамках своих обязанностей данный сотрудник должен:

– осуществлять обработку на АРМ конфиденциальной информации, не относящейся к государственной тайне;

– ознакомиться под роспись и выполнять требования организационно-распорядительной документации на аттестованную ИС (при наличии аттестации);

– выполнять инструкцию пользователя АРМ;

– осуществлять контроль над выполнением требований, перечисленных в пункте 4 настоящего документа;

– оповещать администратора безопасности ИС о любых инцидентах информационной безопасности;

– в случае нарушения и/или невозможности выполнять вышеизложенные требования немедленно прекратить обработку конфиденциальной информации.

4 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 АРМ или администратором информационной безопасности сегмента ИС.

4.1 ТРЕБОВАНИЯ ПО РАЗМЕЩЕНИЮ ТЕХНИЧЕСКИХ СРЕДСТВ

При размещении технических средств необходимо руководствоваться следующими требованиями:

– должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным АРМ, 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;

– АРМ, на которых установлены средства криптографической защиты информации (далее - СКЗИ) должны быть оборудованы средствами контроля за их вскрытием (опломбированы);

– входные двери помещения, в которых ведется обработка информации с использованием СКЗИ, должны быть оборудованы плотно запираемыми дверьми с крепкими замками;

– окна помещений с СКЗИ, находящиеся на первом и последнем этажах, а также вблизи пожарных лестниц должны оснащаться решетками, а сами помещения охранной сигнализацией;

– дистрибутивы и ключевые носители СКЗИ, а также техническая и эксплуатационная документация на СКЗИ должны хранится в запираемых металлических шкафах или сейфах.

4.2 ТРЕБОВАНИЯ ПО УСТАНОВКЕ ОБЩЕСИСТЕМНОГО И СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

На аттестованном АРМ сегмента ИС запрещается установка, удаление, модификация и иные действия с программным обеспечением любым лицом, кроме администратора безопасности сегмента ИС.

4.3 ТРЕБОВАНИЯ К РАЗРАБОТКЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ СЕГМЕНТА ИНФОРМАЦИОННОЙ СИСТЕМЫ

Согласно п.15 документа [8] и п. 6 документа [13] этап разработки системы защиты информации включает в себя проектирование защиты информации и разработку эксплуатационной документации на систему защиты информации.

Результаты проектирования системы защиты информации информационной системы отражаются в эскизном (техническом) и (или) эксплуатационной документации с учетом ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

Эксплуатационная документация на систему защиты информации должна содержать описание:

- структуры системы защиты информации;
- состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
- правил эксплуатации системы защиты информации информационной системы.

Таким образом, при проведении процедуры аттестации сегмента ИС проверяется наличие проектной и эксплуатационной документации на систему защиты информации сегмента ИС.

5 ТРЕБОВАНИЯ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Перечень технических мер защиты информационных систем формируется в соответствии с требованиями [6], [7], [8].

Перечень технических мер защиты для сегмента ИС как минимум должен включает в себя:

- идентификацию и аутентификацию субъектов доступа и объектов доступа (далее – ИАФ) (ИАФ.1; ИАФ.3; ИАФ.4; ИАФ.5; ИАФ.6);
- управление доступом субъектов доступа к объектам доступа (далее – УПД) (УПД.1; УПД.2; УПД.3; УПД.4; УПД.5; УПД.6; УПД.10; УПД.11; УПД.13; УПД.14; УПД.15; УПД.16);
- защиту машинных носителей информации (далее – ЗНИ) (ЗНИ.8);
- регистрацию событий безопасности (далее – РСБ) (РСБ.1; РСБ.2; РСБ.3; РСБ.7);
- антивирусную защиту (далее – АВЗ) (АВЗ.1; АВЗ.2);
- контроль (анализ) защищенности информации (далее – АНЗ) (АНЗ.1; АНЗ.2; АНЗ.3; АНЗ.4);
- защиту среды виртуализации (далее –ЗСВ) (ЗСВ.1; ЗСВ.2; ЗСВ.3; ЗСВ.9; ЗСВ.10);
- защиту технических средств (далее – ЗТС) (ЗТС.3; ЗТС.4);
- защиту информационной системы, ее средств, систем связи и передачи данных (далее – ЗИС) (ЗИС.3; ЗИС.20);
- управление конфигурацией информационной системы и системы защиты персональных данных (далее – УКФ) (УКФ.1, УКФ.2, УКФ.3, УКФ.4);
- криптографическую защиту информации, передаваемой по неконтролируемым каналам связи (СКЗИ).

5.1 ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ АРМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Защита от несанкционированного доступа должна быть обеспечена применением сертифицированного средства защиты от несанкционированного доступа (СЗИ от НСД) – Dallas Lock 8.0-К, оснащенного модулем «межсетевой экран» или аналогичным СЗИ от НСД с модулем «межсетевой экран», имеющим сертификат ФСТЭК России, подтверждающий выполнение требований информационного сообщения ФСТЭК России от 28 апреля 2016 года № 240/24/1986 «Об утверждении требований к межсетевым экранам».

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;

– фильтрацию сетевого трафика.

Установка и настройка СЗИ от НСД проводится на АРМ сегмента ИС в соответствии с эксплуатационной документацией производителя.

5.2 ТРЕБОВАНИЯ К АНТИВИРУСНОЙ ЗАЩИТЕ

Антивирусная защита создается для обеспечения безопасности защищаемой информации и программно-аппаратной среды ИС, 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.;

– «Dr.Web Enterprise Security Suite». Производитель ООО «Доктор Веб». Сертификат ФСТЭК № 3509 от 27.01.2016 г.

Если для работы в сегменте ИС предусмотрено использование съемных носителей информации, то 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 АРМ сегмента ИС должна осуществляться с сертифицированного дистрибутива в соответствии с эксплуатационной документацией производителя.

5.3 ТРЕБОВАНИЯ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ И МЕЖСЕТЕВОМУ ЭКРАНИРОВАНИЮ

Согласно требованиям Постановления Правительства Курганской области от 08.09.2015 г. № 285 «О защищенной сети передачи данных Правительства Курганской области», (далее - ПП Курганской области № 285) при эксплуатации сегмента региональной ИС, организация-претендент для организации защищенного канала связи должна использовать защищенную сеть передачи данных Правительства Курганской области, построенную на технологии ViPNet (**сеть ViPNet № 3335**).

Для организации защищенного канала связи, на АРМ организации-претендента должен быть установлен программный комплекс, выполняющий на рабочем месте пользователя с прикладным ПО функции VPN-клиента, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования ViPNet Client (Производитель ОАО «ИнфоТеКС) 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.

В качестве средства персонального межсетевого экранирования на АРМ пользователей должен быть установлен и настроен модуль «межсетевой экран», входящий в состав СЗИ от НСД Dallas Lock 8.0-K, или аналогичного СЗИ от НСД.

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

5.4 ТРЕБОВАНИЯ К АНАЛИЗУ ЗАЩИЩЕННОСТИ

Подсистема анализа защищенности сегмента ИС должна быть представлена одним из двух сертифицированных ФСТЭК России сканеров безопасности информации:

– XSpider 7.8.25. Производитель - ЗАО «Positive Technologies». Сертификат соответствия ФСТЭК России № 3247 от 24.10.2014 г.

– RedCheck. Производитель - компания «АЛТЭКС-СОФТ». Сертификат соответствия ФСТЭК России № 3172 от 23.06.2014 г.

Сканер безопасности должен выполнять следующие функции:

– идентификация и анализ уязвимостей;

– инвентаризация ресурсов, таких как операционная система, программное обеспечение и устройства сети;

– формирование отчетов, содержащих описание уязвимостей и варианты их устранения.

В ходе эксплуатации аттестованного сегмента ИС установленным интервалом 1 раз в год должен проводится контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в сегменте ИС.

В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляется:

– контроль за событиями безопасности и действиями пользователей в информационной системе;

– контроль (анализ) защищенности информации, содержащейся в информационной системе;

– анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы;

– периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

– контроль соблюдения требований в части эксплуатации СКЗИ.