ПРИЛОЖЕНИЕ №15
УТВЕРЖДЕНО
Приказом «О вводе в действие комплекта организационно-распорядительной документации по организации обработки и защиты персональных данных» МБОУ Сокольская СШ
от «30» августа 20 24 г.
№ 595

(М.П.)

Инструкция
по защите технических средств
информационных систем персональных данных

Оглавление

1. Общие положения

1.1. Муниципальное бюджетное общеобразовательное учреждение Сокольская средняя школа (далее – Организация) руководствуется настоящей Инструкцией по защите технических средств информационных систем персональных данных, определяющей порядок действий администратора безопасности и пользователей информационных систем персональных данных «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании» @ (далее – информационные системы) при защите технических средств информационных систем, в том числе технических средств систем защиты информации.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	**Расшифровка сокращения**
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ПДн	Персональные данные

Таблица 2 – Перечень терминов и определений

Термин	**Определение**	**Источник**
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Контролируемая зона	Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств	ГОСТ Р 56115-2014
Персональные данные	Любая информация, относящаяся	Федеральный закон

Термин	Определение	Источник
	прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,

постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Пользователи информационных систем должны быть ознакомлены с настоящей Инструкцией до начала работы в информационных системах под роспись. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.

2. Определение границ контролируемой зоны

2.1. Границами контролируемой зоны информационных систем являются ограждающие конструкции здания, в котором установлены технические средства информационных систем, в том числе средства защиты информации (внешние границы стен помещений, включая окна и двери).

2.2. Границы контролируемой зоны информационных систем определены приказами Организации.

2.3. Помещения, предназначенные для размещения технических средств информационных систем и средств защиты информации, определены в эксплуатационной документации на системы защиты информации информационных систем и утверждены приказами Организации.

2.4. Перемещение стационарного оборудования информационных систем и средств защиты информации за границу контролируемой зоны не допускается.

2.5. Несанкционированный вынос за границу контролируемой зоны учтенных машинных носителей, мобильных технических средств запрещен.

2.6. Вынос для ремонта за границу контролируемой зоны оборудования информационных систем и средств защиты информации допустим только с письменного разрешения руководителя Организации с учетом выполнения требований Инструкции по защите машинных носителей персональных данных в Организации.

2.7. Несанкционированный внос пользователями информационных систем неучтенных машинных носителей, мобильных технических средств запрещен.

3. Доступ в контролируемую зону

3.1. На период обработки защищаемых ПДн в Помещениях, где размещено оборудование информационных систем средств защиты информации, могут находиться только работники, допущенные к обработке персональных данных в соответствии с утвержденными приказами Организации.

3.2. Доступ в контролируемую зону осуществляется в соответствии с «Порядком доступа в помещения, в которых размещены информационные системы персональных данных».

3.3. Организацию физического доступа в помещения контролируемых зон информационных систем осуществляет ответственный за организацию обработки ПДн.

4. Правила размещения технических средств и устройств вывода информации.

4.1. При размещении в Помещениях технических средств информационных систем, в том числе средств защиты информации, должны быть реализованы меры, направленные на предотвращение случаев несанкционированного вскрытия средств вычислительной техники.

4.2. Корпуса средств вычислительной техники информационных систем опечатываются.

4.3. При размещении в помещениях контролируемых зон средств отображения информации (мониторы и другие средства визуального отображения информации) должен быть исключен несанкционированный просмотр выводимой на них информации.

4.4. Размещение средств отображения информации указано в эксплуатационной документации на информационные системы и эксплуатационной документации на системы защиты информации.

4.5. При обнаружении нарушения целостности пломб ставится в известность администратор безопасности.

4.6. Выполнение требований к размещению устройств вывода информации и контроль целостности пломб в контролируемых зонах обеспечивает администратор безопасности.

5. Защита каналов связи

5.1. Технические средства (кабельные разъемы, маршрутизаторы, сетевой экран и т.п.) для подключения информационных систем к каналам связи, выходящими за пределы контролируемой зоны, должны быть размещены в пределах контролируемой зоны.

5.2. Расположение указанных технических средств и физический доступ к ним контролирует администратор безопасности.

6. Ответственность

Работники Организации несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.