ПРИЛОЖЕНИЕ №8
УТВЕРЖДЕНО
Приказом «О вводе в действие комплекта организационно-распорядительной документации по организации обработки и защиты персональных данных» МБОУ Сокольская СШ
от «____» _____ 20 _____ г.
№ _____
(М.П.)

Положение
о порядке организации и проведении работ
по защите персональных данных, обрабатываемых
в информационных системах персональных данных «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании»

Оглавление

1. Общие положения

1.1 Муниципальное бюджетное общеобразовательное учреждение Сокольская средняя школа (далее – Организация) руководствуется настоящим Положением о порядке организации и проведении работ по защите персональных данных, обрабатываемых в информационной системе персональных данных «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании» (далее – Положение), разработанным в соответствии со следующими нормативными правовыми актами Российской Федерации в области обработки и защиты персональных данных:

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

Постановление Правительства Российской Федерации 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.

1.2 Сокращения, термины и определения

В настоящем Положении 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
Антивирусное ПО	Программное обеспечение средств антивирусной защиты
Вредоносное ПО	Вредоносная компьютерная программа (вирус)
АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
ПО	Программное обеспечение
СВТ	Средства вычислительной техники

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник

Термин	Определение	Источник
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных	
Администратор системный	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы (администратор системный) в соответствии с установленной ролью	
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы	ГОСТ Р 51275-2006
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Инцидент информационной безопасности	Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность	ГОСТ Р ИСО МЭК 27001
(компьютерный) вирус	Вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы	ГОСТ Р 51275-2006
Машинный носитель информации	Материальный носитель, используемый для передачи и хранения защищаемой информации (в том числе персональных данных (далее – ПДн)) в электронном виде.	
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному	Федеральный закон от 27.07.2006 № 152-

Термин	Определение	Источник
	или определяемому физическому лицу (субъекту персональных данных)	ФЗ «О персональных данных»
Событие информационной безопасности	Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью	ГОСТ Р ИСО МЭК 27001

1.3 Администратор безопасности, системный администратор и пользователи ИСПДн должны быть ознакомлены с настоящей Инструкцией до начала работы в ИСПДн под роспись. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.

1.4. Для координации и контроля выполнения мероприятий по обработке и защите персональных данных в Организации назначается должностное лицо, ответственное за организацию обработки персональных данных.

При выполнении своих обязанностей ответственный за организацию обработки персональных данных руководствуется требованиями «Инструкции ответственного за организацию обработки персональных данных».

1.5 В Организации утверждены «Правила обработки персональных данных информационных систем персональных данных «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании»» в целях:

- обеспечения защиты прав и свобод субъектов персональных данных при обработке персональных данных в Организации;

- установления процедур, направленных на выявление и предотвращение нарушений законодательства Российской Федерации о персональных данных, иных правовых актов Российской Федерации, внутренних документов Организации по вопросам обработки и защиты персональных данных;

- определения целей обработки персональных данных в информационных системах персональных данных «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании» в установленной сфере деятельности, включая содержание обрабатываемых персональных данных, категории субъектов персональных данных, данные которых обрабатываются, сроки обработки (в том числе хранения)

обрабатываемых персональных данных, а также порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований;

- установления ответственности работников Организации, имеющих доступ к персональным данным субъектов персональных данных в информационных системах персональных данных «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании» за невыполнение требований норм, регулирующих обработку персональных данных, установленных законодательством Российской Федерации, настоящими Правилами и иными локальными актами Организации.

1.6 Для непосредственного выполнения работ по защите персональных данных с использованием программно-аппаратных средств защиты информации (далее – СЗИ) назначается лицо, ответственное за обеспечение безопасности персональных данных в информационной системе персональных данных (далее – администратор безопасности)

При выполнении своих обязанностей, администратор безопасности действует в соответствии с требованиями «Инструкции администратора безопасности информационных систем персональных данных» и требованиями эксплуатационной документации на средства защиты информации, используемые в составе системы защиты информации.

1.7 Все пользователи ИСПДн участвуют в защите персональных данных, содержащейся в ИСПДн, и обязаны знать и выполнять требования:

- нормативных правовых документов Российской Федерации по защите информации, в том числе по защите персональных данных;
- настоящего Положения и перечисленных в нём инструкций, в части их касающейся;
- «Инструкция пользователя информационных систем персональных данных».

1.8 В ходе эксплуатации информационных систем персональных данных «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании» защита персональных данных обеспечивается выполнением процедур:

- управления (администрирования) системой защиты информации в ИСПДн;
- контроля обеспечения уровня защищённости персональных данных в ИСПДн.

2. Управление системой защиты персональных данных ИСПДн «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании»

2.1 Процедуры управления системой защиты персональных данных обеспечивают:

- функционирование системы защиты персональных данных ИСПДн в штатном режиме с характеристиками, установленными в проектной документации;
- документированный поток информации о событиях безопасности в ИСПДн и её системе защиты, на основании которой возможна реализация процедур управления инцидентами, процедуры контроля уровня защищённости персональных данных, обрабатываемых в ИСПДн.

2.2 Порядок действий пользователей ИСПДн при прохождении процедур идентификации (узнавании) и аутентификации (подтверждении подлинности узнанного пользователя) при входе в ИСПДн описаны в «Инструкции по идентификации и аутентификации пользователей информационных систем персональных данных».

2.3. Порядок управления доступом пользователей к информационным ресурсам ИСПДн устанавливается в «Инструкции по управлению доступом к информационным системам персональных данных».

2.4. Порядок действий пользователей ИСПДн при работе с машинными носителями персональных данных, правила учёта, хранения и доступа к машинным носителям описаны в «Инструкции по защите машинных носителей персональных данных».

2.5 Порядок действий администратора безопасности и системных администраторов ИСПДн при появлении событий безопасности описаны в «Инструкции по управлению событиями информационной безопасности информационных систем персональных данных».

2.6 Порядок действий пользователей при обнаружении вредоносного ПО, описаны в «Инструкции по антивирусной защите информационных систем персональных данных».

2.7 Порядок действий системных администраторов и администратора безопасности ИСПДн с целью:

- выявления ошибок и недостатков программного обеспечения и аппаратных средств, и средств защиты персональных данных ИСПДн;
- контроля установки обновлений программного обеспечения, контроля работоспособности и настроек программного обеспечения;
- контроля состава технических и программных средств ИСПДн, в том числе средств защиты информации, описан в «Инструкция по контролю (анализу) защищенности персональных данных информационных систем персональных данных».

2.8 Порядок доступа пользователей к техническим средствам ИСПДн и СЗИ, описан в «Инструкции по защите технических средств информационных систем персональных данных».

2.9 Организация резервного копирования и восстановления персональных данных в ИСПДн осуществляется администратором безопасности с заданной периодичностью, определяемой Регламентом резервного копирования (при наличии).

2.10 Организация режима безопасности помещений, в которых размещена ИСПДн, правила доступа в помещения в рабочее, нерабочее время и в нештатных ситуациях определены в «Порядке доступа в помещения, в которых размещены информационные системы персональных данных».

2.11 Обеспечение безопасности персональных данных при обработке в ИСПДн с использованием средств криптографической защиты информации осуществляется в соответствии с «Положением по использованию средств криптографической защиты информации», «Порядком доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств, «Инструкцией пользователя средств криптографической защиты информации», «Инструкцией ответственного пользователя средств криптографической защиты информации»

3. Контроль обеспечения уровня защищённости персональных данных ИСПДн «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании»

3.1 Периодичность контроля обеспечения уровня защищённости персональных данных, обрабатываемых в ИСПДн, составляет 1 год.

3.2. Для контроля обеспечения уровня защищённости используются следующие документы:

- отчёты о событиях информационной безопасности;
- результаты контроля защищённости;
- информация из специальных источников по новым угрозам безопасности для используемых в ИСПДн программных и программно – технических средств.

3.2 На основе указанных выше документов, ответственный за организацию обработки персональных данных:

- анализ функционирования системы защиты информации, включая сбои и неисправности аппаратно-программных средств защиты информации;
- анализ изменения угроз безопасности персональных данных, обрабатываемых в ИСПДн

3.3 К анализу привлекаются системные администраторы и администратор безопасности. По отдельному договору к анализу могут быть привлечены специалисты сторонних организаций.

3.4 Ответственный за организацию обработки персональных данных организует документирование результатов проведённого анализа в виде Акта контроля обеспечения защищённости персональных данных.

3.5 На основании выводов Акта контроля защищённости персональных данных, ответственный за организацию обработки персональных данных при необходимости доработки системы защиты персональных данных докладывает об этом руководителю Организации. Решение о доработке и последующей аттестации принимает руководитель Организации.

4. Ответственность

4.1 Пользователи ИСПДн должны быть предупреждены об ответственности за действия персональными данными, содержащимися в ИСПДн и действия с техническими средствами ИСПДн и СЗИ, нарушающие требования настоящего Положения и других организационно-распорядительных документов, определяющих меры по защите персональных данных в ИСПДн «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании».