«УТВЕРЖДАЮ»
Директор МБОУ
«Средняя общеобразовательная школа №16»
_____ Е.В. Кабанова
«24» апреля 2015 года

ОТЧЁТ
О РЕЗУЛЬТАТАХ ПРОВЕДЕНИЯ ВНУТРЕННЕЙ ПРОВЕРКИ

Сергиев Посад
2015

транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и/или выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов, персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующими описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование и уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и/или осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы

и другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и/или блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокиро-

вание, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – образовательное учреждение города Сергиев Посад.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС	-	антивирусные средства
АИС	-	автоматизированная информационная система
АРМ	-	автоматизированное рабочее место
ИНН	-	индивидуальный номер налогоплательщика
ИСПДн	-	информационная система персональных данных
ЛВС	-	локальная вычислительная сеть
ЛИС	-	локальная информационная система
МЭ	-	межсетевой экран
НСД	-	несанкционированный доступ
ОС	-	операционная система
ПДн	-	персональные данные
ПМВ	-	программно-математическое воздействие
ПО	-	программное обеспечение
ПФ	-	пенсионный фонд
ПЭМИН	-	побочные электромагнитные излучения и наводки
РИС	-	распределенная информационная система
СЗИ	-	средства защиты информации
СЗПДн	-	система (подсистема) защиты персональных данных
ТКУИ	-	технические каналы утечки информации
УБПДн	-	угрозы безопасности персональных данных
БД		Базы данных
СУБД		Система управления базой данных
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю – федеральный орган исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

1.5. Угрозы безопасности ПДн

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

1. Угрозы от утечки по техническим каналам:
   1.1. Угрозы утечки акустической информации;
   1.2. Угрозы утечки видовой информации;
   1.3. Угрозы утечки информации по каналам ПЭМИН.
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа:
   2.1. Кража и уничтожение носителей информации;
   2.2. Кража физических носителей ключей и атрибутов доступа;
   2.3. Утрата носителей информации;
   2.4. Утрата и компрометация ключей и атрибутов доступа.
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств:
   3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа;
   3.2. Утечка информации через порты ввода/вывода;
   3.3. Воздействие вредоносных программ (вирусов);
   3.4. Установка ПО, не связанного с исполнением служебных обязанностей;
   3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных;
   3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему.
4. Угрозы несанкционированного доступа к информации по каналам связи:
   4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны;
   4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
   4.3. Угрозы выявления паролей по сети;
   4.4. Угрозы типа «Отказ в обслуживании»;
   4.5. Угрозы внедрения по сети вредоносных программ;
   4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа;
   4.7. Перехват, модификация закрытого ключа ЭЦП;
   4.8. Угрозы удаленного запуска приложений.
5. Угрозы антропогенного характера:
   5.1. Разглашение информации;
   5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов;
   5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей;
   5.4. Угроза нарушения политики предоставления и прекращения доступа;
   5.5. Непреднамеренная модификация (уничтожение) информации;
   5.6. Непреднамеренное отключение средств защиты.
6. Угрозы воздействия непреодолимых сил:
   6.1. Стихийное бедствие;
   6.2. Выход из строя аппаратно-программных средств;
   6.3. Аварии (пожар, потоп, случайное отключение электричества).

Анализ вероятности реализации, реализуемости, опасности и актуальности угроз представлен в Модели угроз.

1.6. Существующие меры защиты

Существующие в ИСПДн технические меры защиты представлены в таблице 4.

Таблица 4

Технические меры защиты

Элемент ИСПДн	Программное средство обработки ПДн	Установленные средства защиты
АРМ пользователя	ОС Windows Браузер IE	Средства ОС: - управление и разграничение доступа пользователей; - регистрация и учет действий с информацией; - ПО «Антивирус Касперского»; - обеспечение целостности данных; - обнаружение вторжений.
СпецПО и СУБД	1С: Бухгалтерия (платформа 1С: Предприятие 8.2)	Средства БД. Средства ОС: - управление и разграничение доступа пользователей; - регистрация и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.

В ИСПДн введены следующие организационные меры защиты:

- в Учреждении осуществляется контроль доступа в контролируемую зону - двери закрываются на замок;
- ведется учет носителей информации;
- носители информации хранятся в сейфе;
- в Учреждении существует ответственный сотрудник за обеспечение безопасности ПДн;
- в Учреждении проводятся периодические внутренние проверки режима безопасности ПДн;
- введена парольная политика, устанавливающая сложность ключей и атрибутов доступа (паролей), а также их периодическую смену;
- пользователи осведомлены и проинструктированы о порядке работы и защиты персональных данных;
- осуществляется резервное копирование защищаемой информации;
- в помещениях, где расположены элементы ИСПДн, установлена автоматическая пожарная сигнализация.

1.7. Необходимые меры защиты

На основании анализа актуальности выявленных угроз безопасности, для достижения требуемого уровня защиты рекомендуется осуществить следующие мероприятия:

- установка антивирусной защиты;
- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;
- назначение ответственного за безопасность персональных данных из числа сотрудников учреждения;
- разработка и утверждение инструкций пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а также с ключами и атрибутами доступа;
- осуществление резервирования ключевых элементов ИСПДн;
- изоляция портов ввода/вывода;
- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.

2. ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ «МЕЖВЕДОМСТВЕННАЯ СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА» (МСЭД)

2.1. Структура ИСПДн

Таблица 5

Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Автоматизированное рабочее место
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская
Режим разграничения прав доступа пользователей	Система с разграничением доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Дополнительная информация	К персональным данным предъявляется требование целостности и (или) доступности

2.2. Состав и структура персональных данных

В ИСПДн обрабатываются следующие персональные данные:
- ФИО работников;
- табельный номер;
- номера домашнего и мобильного телефонов;
- ФИО обучающихся;
- дата рождения;
- номер паспорта;
- ИНН, номер полиса пенсионного страхования;
- номер полиса ОМС.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **4 категории персональных данных,** т.е. к данным, не позволяющим идентифицировать субъекта персональных данных.

Объем обрабатываемых персональных данных **не превышает 1500 записей** о субъектах персональных данных.

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, на основании категории и объема обрабатываемых персональных данных – **ИСПДн *«МЕЖВЕДОМСТВЕННАЯ СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА» (МСЭД)* классифицируется как специальная ИСПДн класса К4.**

Так же в ИСПДн существуют следующие объекты защиты:
- технологическая информация:
  - управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
  - технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
  - информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;

- информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки обрабатываемой информации.

- технические средства обработки:
  - общее и специальное программное обеспечение, участвующее в обработке ПДн (операционные системы, СУБД, клиент-серверные приложения и другие);
  - резервные копии общесистемного программного обеспечения;
  - инструментальные средства и утилиты систем управления ресурсами ИСПДн;
  - аппаратные средства обработки ПДн (АРМ и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.);
- средства защиты ПДн:
  - средства управления и разграничения доступа пользователей;
  - средства обеспечения регистрации и учета действий с информацией;
  - средства, обеспечивающие целостность данных;
  - средства антивирусной защиты;
  - средства межсетевого экранирования;
  - средства анализа защищенности;
  - средства обнаружения вторжений;
  - средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

2.3. Структура обработки ПДн

В ИСПДн ***«МЕЖВЕДОМСТВЕННАЯ СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА» (МСЭД)*** обработка персональных данных происходит следующим образом:

- работник авторизуется на своем рабочем месте в ОС Windows;
- работник авторизуется в ПО *«МЕЖВЕДОМСТВЕННАЯ СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА» (МСЭД);*
- работник вносит персональные данные об обучающихся или о работников;
- данные хранятся в БД на АРМ.

2.4. Режим обработки ПДн

В ИСПДн ***«МЕЖВЕДОМСТВЕННАЯ СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА» (МСЭД)*** обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в таблице 6.

Таблица 6

Список типовых ролей (матрица доступа)

Группа	Уровень доступа к ПДн	Разрешенные действия	Работники учреждения
Администратор ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Инженер ПЭВМ
Администратор безопасности	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Инженер ПЭВМ
Операторы ИСПДн с правами записи и чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Заместитель директора школы по УВР Секретарь директора школы

Перечень работников, осуществляющих работу в ИСПДн представлен в таблице 7.

Таблица 7

Перечень работников, осуществляющих работу в ИСПДн

№ п/п	Роль	ФИО сотрудника	Подразделение
1	Администратор ИСПДн	Савва В.И.	инженер ПЭВМ
2	Оператор	Гладун А.Н.	секретарь директора школы

2.5. Угрозы безопасности ПДн

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

1. Угрозы от утечки по техническим каналам:
   1.1. Угрозы утечки акустической информации;
   1.2. Угрозы утечки видовой информации;
   1.3. Угрозы утечки информации по каналам ПЭМИН.
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа:
   2.1. Кража и уничтожение носителей информации;
   2.2. Кража физических носителей ключей и атрибутов доступа;
   2.3. Утрата носителей информации;
   2.4. Утрата и компрометация ключей и атрибутов доступа.
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств:
   3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа;
   3.2. Утечка информации через порты ввода/вывода;
   3.3. Воздействие вредоносных программ (вирусов);
   3.4. Установка ПО, не связанного с исполнением служебных обязанностей;
   3.5. Внедрение или сокрытие не декларированных возможностей системного ПО и ПО для обработки персональных данных;
   3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему.
4. Угрозы несанкционированного доступа к информации по каналам связи:
   4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны;
   4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
   4.3. Угрозы выявления паролей по сети;
   4.4. Угрозы типа «Отказ в обслуживании»;
   4.5. Угрозы внедрения по сети вредоносных программ;
   4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа;
   4.7. Перехват, модификация закрытого ключа ЭЦП;
   4.8. Угрозы удаленного запуска приложений.
5. Угрозы антропогенного характера:
   5.1. Разглашение информации;
   5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов;
   5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей;
   5.4. Угроза нарушения политики предоставления и прекращения доступа;
   5.5. Непреднамеренная модификация (уничтожение) информации;
   5.6. Непреднамеренное отключение средств защиты.
6. Угрозы воздействия непреодолимых сил:
   6.1. Стихийное бедствие;
   6.2. Выход из строя аппаратно-программных средств;
   6.3. Аварии (пожар, потоп, случайное отключение электричества).

Анализ вероятности реализации, реализуемости, опасности и актуальности угроз представлен в Модели угроз.

2.6. Существующие меры защиты

Существующие технические меры защиты в ИСПДн представлены в таблице 8.

Таблица 8

Технические меры защиты в ИСПДн

Элемент ИСПДн	Программное средство обработки ПДн	Установленные средства защиты
АРМ пользователя	ОС Windows Браузер IE	Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией; - ПО «Антивирус Касперского»; - регистрация и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.
СпецПО и СУБД	Типовое ядро уровня ОУ	Средства БД Средства ОС: - управление и разграничение доступа пользователей; - регистрация и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.

В ИСПДн введены следующие организационные меры защиты:

- в Учреждении осуществляется контроль доступа в контролируемую зону, двери закрываются на замок;
- ведется учет носителей информации;
- носители информации хранятся в сейфе;
- в Учреждении ответственный сотрудник за обеспечение безопасности ПДн;
- в Учреждении проводятся периодические внутренние проверки режима безопасности ПДн;
- введена парольная политика, устанавливающая сложность ключей и атрибутов доступа (паролей), а также их периодическую смену;
- пользователи осведомлены и проинструктированы о порядке работы и защиты персональных данных;
- осуществляется резервное копирование защищаемой информации;
- в помещениях, где расположены элементы ИСПДн, установлена пожарная сигнализация.

2.7. Необходимые меры защиты

На основании анализа актуальности выявленных угроз безопасности, для достижения требуемого уровня защиты рекомендуется осуществить следующие мероприятия:

- установка антивирусной защиты;
- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;
- назначение ответственного за безопасность персональных данных из числа работников учреждения;
- разработка инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а также с ключами и атрибутами доступа;
- осуществление резервирования ключевых элементов ИСПДн;
- изолирование портов ввода/вывода;
- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.

3. ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ «ШКОЛЬНЫЙ ПОРТАЛ МОСКОВСКОЙ ОБЛАСТИ»

3.1. Структура ИСПДн

Таблица 9

Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Автоматизированное рабочее место
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская
Режим разграничения прав доступа пользователей	Система с разграничением доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Дополнительная информация	К персональным данным предъявляется требование целостности и (или) доступности

3.2. Состав и структура персональных данных

В ИСПДн обрабатываются следующие персональные данные:
- ФИО работников;
- номера домашнего и мобильного телефонов;
- ФИО обучающихся;
- дата рождения;
- номер паспорта;
- ИНН, номер полиса пенсионного страхования;
- номер полиса ОМС.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **4 категории персональных данных,** т.е. к данным, не позволяющим идентифицировать субъекта персональных данных.

Объем обрабатываемых персональных данных **не превышает 1500 записей** о субъектах персональных данных.

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, на основании категории и объема обрабатываемых персональных данных – **ИСПДн** *«Школьный портал Московской области»* **классифицируется как специальная ИСПДн класса К4.**

Так же в ИСПДн существуют следующие объекты защиты:
- технологическая информация:
  - информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
  - информация о СЗПДн, структуре, принципах и технических решениях защиты;
- технические средства обработки:
  - аппаратные средства обработки ПДн (АРМ и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.);
- средства защиты ПДн:
  - средства управления и разграничения доступа пользователей;
  - средства обеспечения регистрации и учета действий с информацией;
  - средства, обеспечивающие целостность данных;
  - средства антивирусной защиты;
  - средства межсетевого экранирования;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

3.3. Структура обработки ПДн

В ИСПДн *«Школьный портал Московской области»* обработка персональных данных происходит следующим образом:

- работник авторизуется на своем рабочем месте в ОС Windows;
- работник авторизуется на «Школьном портале Московской области»;
- работник вносит персональные данные об учащихся или о работниках;
- данные хранятся в БД на Сервере «Школьного портала Московской области». В ИСПДн «Школьного портала Московской области» обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в таблице 10.

Таблица 10

Список типовых ролей представлен (матрица доступа)

Группа	Уровень доступа к ПДн	Разрешенные действия	Работники учреждения
Администратор ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Учитель информатики, Учитель начальных классов
Администратор безопасности	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Учитель информатики, Учитель начальных классов
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Заместители директора школы по УВР Классные руководители Учителя предметники
Операторы ИСПДн с правами чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн.	- использование	Родители обучающихся Обучающиеся

Перечень работников, осуществляющих работу в ИСПДн представлен в таблице 11.

Таблица 11

Перечень работников, осуществляющих работу В ИСПДн

№ п/п	Роль	ФИО сотрудника	Подразделение
1	Администратор ИСПДн	Романенко О.А., Шарикова Е.А.	Учитель информатики, Учитель начальных классов
2	Оператор	Сафронова Ю.А.	Заместитель директора школы по УВР
3	Классные руководители, учителя предметники, работники администрации школы.	Согласно утвержденному директором школы списку	

3.4. Угрозы безопасности ПДн

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

1. Угрозы от утечки по техническим каналам:
   1.1. Угрозы утечки акустической информации;
   1.2. Угрозы утечки видовой информации;
   1.3. Угрозы утечки информации по каналам ПЭМИН.
2. Угрозы несанкционированного доступа к информации путем физического доступа к элементам ИСПДн, носителям персональных данных, ключам и атрибутам доступа:
   2.1. Кража и уничтожение носителей информации;
   2.2. Кража физических носителей ключей и атрибутов доступа;
   2.3. Утрата носителей информации;
   2.4. Утрата и компрометация ключей и атрибутов доступа.
3. Угрозы несанкционированного доступа к информации с использованием программно-аппаратных и программных средств:
   3.1. Доступ к информации, ее модификация и уничтожение лицами, не имеющими прав доступа;
   3.2. Утечка информации через порты ввода/вывода;
   3.3. Воздействие вредоносных программ (вирусов);
   3.4. Установка ПО, не связанного с исполнением служебных обязанностей;
   3.5. Внедрение или сокрытие недекларированных возможностей системного ПО и ПО для обработки персональных данных;
   3.6. Создание учетных записей теневых пользователей и неучтенных точек доступа в систему.
4. Угрозы несанкционированного доступа к информации по каналам связи:
   4.1. Угроза «Анализ сетевого трафика» с перехватом информации за пределами контролируемой зоны;
   4.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
   4.3. Угрозы выявления паролей по сети;
   4.4. Угрозы типа «Отказ в обслуживании»;
   4.5. Угрозы внедрения по сети вредоносных программ;
   4.6.Утечка информации, передаваемой с использованием протоколов беспроводного доступа;
   4.7. Перехват, модификация закрытого ключа ЭЦП;

4.8. Угрозы удаленного запуска приложений.

5. Угрозы антропогенного характера:

5.1. Разглашение информации;

5.2. Сокрытие ошибок и неправомерных действий пользователей и администраторов;

5.3. Угроза появления новых уязвимостей вследствие невыполнения ответственными лицами своих должностных обязанностей;

5.4. Угроза нарушения политики предоставления и прекращения доступа;

5.5. Непреднамеренная модификация (уничтожение) информации;

5.6. Непреднамеренное отключение средств защиты.

6. Угрозы воздействия непреодолимых сил:

6.1. Стихийное бедствие;

6.2. Выход из строя аппаратно-программных средств;

6.3. Аварии (пожар, потоп, случайное отключение электричества).

Анализ вероятности реализации, реализуемости, опасности и актуальности угроз представлен в Модели угроз.

3.5. Существующие меры защиты

Существующие технические меры защиты в ИСПДн представлены в таблице 12.

Таблица 12

Технические меры защиты в ИСПДн

Элемент ИСПДн	Программное средство обработки ПДн	Установленные средства защиты
АРМ пользователя	ОС Windows Браузер IE	Средства ОС: - управление и разграничение доступа пользователей; - регистрация и учет действий с информацией. ПО «Антивирус Касперского» - регистрация и учет действий с информацией; - обеспечивать целостность данных; - производить обнаружение вторжений.
Сервер	Типовое ядро уровня ОУ	Средства СУБД Средства ОС: - управление и разграничение доступа пользователей; - регистрация и учет действий с информацией; - обеспечение целостности данных; - производить обнаружение вторжений.

В ИСПДн введены следующие организационные меры защиты:

- в Учреждении осуществляется контроль доступа в контролируемую зону, двери закрываются на замок;
- ведется учет носителей информации;
- носители информации хранятся в сейфе;
- в Учреждении существует ответственный работник за обеспечение безопасности ПДн;
- в Учреждении проводятся периодические внутренние проверки режима безопасности ПДн;

- введена парольная политика, устанавливающая сложность ключей и атрибутов доступа (паролей), а также их периодическую смену;

- пользователи осведомлены и проинструктированы о порядке работы и защиты персональных данных;

- осуществляется резервное копирование защищаемой информации;

- в помещениях, где расположены элементы ИСПДн, установлена автоматическая пожарная сигнализация.

3.6. Необходимые меры защиты

На основании анализа актуальности выявленных угроз безопасности, для достижения требуемого уровня защиты рекомендуется осуществить следующие мероприятия:

- установка антивирусной защиты;

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

- назначить ответственного за безопасность персональных данных из числа работников учреждения;

- разработать и утвердить инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а также с ключами и атрибутами доступа;

- осуществить резервирование ключевых элементов ИСПДн;

- изолирование портов ввода/вывода;

- организовать разграничение прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.

Председатель комиссии,
заместитель директора школы по БП — В.Н. Стетюха
Члены комиссии:
учитель информатики — О.А. Романенко
учитель информатики — Л.К. Гришина
инженер ПЭВМ — В.И. Савва