



УТВЕРЖДАЮ
Директор Краснопереконского
психоневрологического интерната

 **М.В. Филиппова**

« 04 » 05 20 17 г.

ОТЧЁТ
о результатах проведения внутренней проверки

Ярославль

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	3
ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ.....	8
ВВЕДЕНИЕ	9
1 ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ "СМЕТА 3.2 БУХГАЛТЕРИЯ».....	10
1.1 Структура ИСПДн.....	10
1.2 Состав и структура персональных данных	10
1.3 Структура обработки ПДн.....	12
1.4 Режим обработки ПДн.....	12
1.5 Угрозы безопасности ПДн	14
1.6 Существующие меры защиты	15
1.7 Необходимые меры защиты.....	16
2 ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ «СМЕТА 3.2 КАДРЫ»	18
2.1 Структура ИСПДн.....	18
2.2 Состав и структура персональных данных	18
2.3 Структура обработки ПДн.....	20
2.4 Режим обработки ПДн.....	20
2.5 Угрозы безопасности ПДн	22
2.6 Существующие меры защиты	24
2.7 Необходимые меры защиты.....	25
3 ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ «VIPNET.CLIENT».....	26
3.1 Структура ИСПДн.....	26
3.2 Состав и структура персональных данных	26
3.3 Структура обработки ПДн.....	28
3.4 Режим обработки ПДн.....	28
3.5 Угрозы безопасности ПДн	30
3.6 Существующие меры защиты.....	32
3.7 Необходимые меры защиты.....	33

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и / или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрический сигнал, акустические, электромагнитные и другие физические поля, по параметрам которых может быть

раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также 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 каж-

дого 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 электромаг-

нитные 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, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и / или заблокировать 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, блокирование, 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 Москвы.

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
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.

ВВЕДЕНИЕ

Внутренняя проверка (далее – Проверка) произведена на основании Приказа № 83/1 от 24.04.18 г.

Проверка проводилась с «24» 04 по «28» 04 г. на территории ГБУ СО ЯО Краснопереконского психоневрологического интерната связи по адресу: 150002, г. Ярославль, ул. Парковый проезд, д. 7.

Проверка проводилась в соответствии с принципами и положениями Концепции информационной безопасности и Политики информационной безопасности учреждения.

В ходе проверки были выявлены следующие ИСПДн:

- «Смета 3.2 «бухгалтерия»
- «Смета 3.2 «кадры»
- «VipNet.Client»

В ходе проверки для каждой ИСПДн определялось:

- состав и структура объектов защиты;
- конфигурация и структура ИСПДн;
- режим обработки ПДн;
- перечень лиц участвующих в обработке ПДн;
- права доступа лиц, допущенных к обработке ПДн;
- угрозы безопасности персональных данных. Оценивалась вероятность их реализации, реализуемость, опасность и актуальность;
- существующие меры защиты ПДн;
- список необходимых мер защиты ПДн.

Данные Проверки служат основой для других нормативно-организационных документов.

Данные о составе и структуре объектов защиты отражаются в Перечне персональных данных, подлежащих защите.

Данные о составе и структуре обрабатываемых персональных данных, конфигурации ИСПДн и режиме обработке являются основой для составления Акта классификации информационной системы, обрабатывающей персональные данные.

Данные о лицах, допущенных к обработке ПДн, и уровне их доступа отражаются в Положении о разграничении прав доступа к обрабатываемым персональным данным.

Данные об угрозах безопасности ПДн служат основой для составления Модели угроз безопасности персональных данных.

Данные о существующих и необходимых мерах защиты ПДн служат основой для составления Плана мероприятий по обеспечению защиты ПДн.

1 ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ «СМЕТА 3.2. «БУХГАЛТЕРИЯ»

1.1 СТРУКТУРА ИСПДн

Таблица 1. 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 без разграничения 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

1.2 СОСТАВ И СТРУКТУРА ПЕРСОНАЛЬНЫХ ДАННЫХ

В ИСПДн обрабатываются следующие персональные данные:

- паспортные данные сотрудников;
- должность;
- оклад.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к 3 категории персональных данных, т.е. к данным, позволяющим идентифицировать субъекта персональных данных.

Объем обрабатываемых персональных данных, не превышает 1000 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 «Смета 3.2 «бухгалтерия»» классифицируется как специальная ИСПДн класса КЗ.

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 Обработываемой информации.
- технические средства обработки:
 - общее и специальное программное обеспечение, участвующее в обработке ПДн (операционные системы);
 - 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.

1.3 СТРУКТУРА ОБРАБОТКИ ПДн

В ИСПДн «Смета 3.2 «бухгалтерия» обработка персональных данных происходит следующим образом:

- сотрудник авторизуется на своем рабочем месте в ОС Microsoft Windows XP;
- сотрудник авторизуется в «Смета 3.2 «бухгалтерия»;
- сотрудник вносит персональные данные о сотрудниках;
- данные хранятся в БД на АРМ.

1.4 РЕЖИМ ОБРАБОТКИ ПДн

В ИСПДн «Смета 3.2 «бухгалтерия» обработка персональных данных осуществляется в многопользовательском режиме без разграничения 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.

Таблица 2. Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия
Администраторы ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфи-	– сбор – систематизация – накопление – хранение

	гурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	– уточнение – использование – уничтожение
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
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	– сбор – систематизация – накопление – хранение – уточнение – использование – уничтожение
Операторы ИСПДн с правами чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн.	– использование

В ИСПДн осуществляют работу следующие сотрудники:

Таблица 3. Перечень сотрудников

№	Роль	ФИО сотрудника	Подразделение
	Администратор ИСПДн	Переверзева Т.А.	Бухгалтерия
	Оператор	Карасева С.А.	Бухгалтерия

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 недеklarированных 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. Соккрытие 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 ниже.

Таблица 4. Меры защиты

Элемент ИСПДн	Программное средство обработки ПДн	Установленные средства защиты
АРМ пользователя	ОС Windows XP Браузер	Средства ОС: управление и разграничение доступа пользователей; регистрацию и учет действий с информацией. ПО «Антивирус Касперского» регистрацию и учет действий с информацией; обеспечивать целостность данных;

		производить обнаружений вторжений.
СпецПО и СУБД	Смета 3.2	Средства БД Средства ОС: управление и разграничение доступа пользователей; регистрацию и учет действий с информацией; обеспечивать целостность данных; производить обнаружений вторжений.

В ИСПДн введены следующие организационные меры защиты:

- в Учреждении осуществляется контроль доступа в контролируемую зону, установлена охранный сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания;
- ведется учет носителей информации;
- носители информации хранятся в сейфе;
- в Учреждении существует отдел/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 так же 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.

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

- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же 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.

2 ИНФОРМАЦИОННАЯ СИСТЕМА, ОБРАБАТЫВАЮЩАЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ «СМЕТА 3.2 «КАДРЫ»

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 сотрудников;
- табельный номер;
- номера домашнего и мобильного телефонов;
- дата рождения;
- номер паспорта;
- ИНН, номер полиса пенсионного страхования;
- Семейное положение;
- Документы об образовании.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к 3 категории персональных данных, т.е. к данным, позволяющим идентифицировать субъекта персональных данных.

Объем обрабатываемых персональных данных, не превышает 1000 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 «Смета 3.2 «кадры»» классифицируется как специальная ИСПДн класса КЗ.

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 «Смета 3.2 «кадры» обработка персональных данных происходит следующим образом:

- сотрудник авторизуется на своем рабочем месте в ОС Windows XP, Windows Vista или Windows 7;
- сотрудник авторизуется в ПО «Смета 3.2 «кадры»;
- сотрудник вносит персональные данные об сотрудниках;
- данные хранятся в БД на АРМ.

2.4 РЕЖИМ ОБРАБОТКИ ПДн

В ИСПДн «Смета 3.2 «кадры» 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.

Таблица 6. Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники отдела
Администраторы 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	Служба информатизации
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 конфигу-	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	

	рированию технических средств сети за исключением контрольных (инспекционных).		
Операторы ИС-ПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Зам. директора по УПР Медиаспециалисты Секретарь-диспетчер учебной части Секретарь приёмной комиссии Сотрудники отдела кадров
Операторы ИС-ПДн с правами чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн.	- использование	Сотрудники отдела кадров

В ИСПДн осуществляют работу следующие сотрудники.

Таблица 7. Перечень сотрудников

№	Роль	ФИО сотрудника	Подразделение
	Администратор ИС-ПДн		
	Оператор	Кононова Т.Г	Кадры
	Оператор	Ячменева О.А.	Кадры

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 недеklarированных 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 в ИСПДн технические меры защиты представлены в таблице ниже.

Таблица 8. Меры защиты

Элемент ИСПДн	Программное средство обработки ПДн	Установленные средства защиты
АРМ пользователя	ОС Windows Браузер	Средства ОС: – управление и разграничение доступа пользователей; – регистрацию и учет действий с информацией. ПО «Антивирус Касперского» – регистрацию и учет действий с информацией; – обеспечивать целостность данных; – производить обнаружений вторжений.
СпецПО и СУБД	Типовое ядро уровня ОУ	Средства БД Средства ОС: – управление и разграничение доступа пользователей; – регистрацию и учет действий с информацией;

		– обеспечивать целостность данных; – производить обнаружений вторжений.
--	--	--

В ИСПДн введены следующие организационные меры защиты:

- в Учреждении осуществляется контроль доступа в контролируемую зону, установлена охранный сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания;
- ведется учет носителей информации;
- носители информации хранятся в сейфе;
- в Учреждении существует отдел/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 так же 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;
- назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;
- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же 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 «VIPNET. CLIENT»

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	Однопользовательская
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 клиентов;
- дата рождения;
- номер паспорта;
- ИНН, номер полиса пенсионного страхования;
- Номер полиса ОМС.
- Адрес регистрации
- Индивидуальная программ.

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к 3 категории персональных данных, т.е. к данным, позволяющим идентифицировать субъекта персональных данных.

– Объем обрабатываемых персональных данных, не превышает 1000 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 «VIPNET. CLIENT» классифицируется как специальная ИСПДн класса К3.

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.

3.3 СТРУКТУРА ОБРАБОТКИ ПДн

В ИСПДн «VIPNET. CLIENT» обработка персональных данных происходит следующим образом:

- сотрудник авторизуется на своем рабочем месте в ОС Windows XP, Windows Vista или Windows 7;
- сотрудник авторизуется в «VIPNET. CLIENT»;
- сотрудник вносит персональные данные об клиентах;
- данные хранятся в БД на Сервере «VIPNET. CLIENT».

3.4 РЕЖИМ ОБРАБОТКИ ПДн

В ИСПДн «VIPNET. CLIENT» 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.

Таблица 10. Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники отдела
Администраторы 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	Служба информатизации
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 конфигу-	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	

	рированию технических средств сети за исключением контрольных (инспекционных).		
Операторы ИС-ПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Специалист по соц. работе
Операторы ИС-ПДн с правами чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн.	- использование	

В ИСПДн осуществляют работу следующие сотрудники.

Таблица 11. Перечень сотрудников

№	Роль	ФИО сотрудника	Подразделение
	Администратор ИС-ПДн		Служба информатизации
	Оператор	Савельева Е.Д.	Спец. по соц. работе

3.5 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 недеklarированных 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. Соккрытие 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.

3.6 СУЩЕСТВУЮЩИЕ МЕРЫ ЗАЩИТЫ

Существующие в ИСПДн технические меры защиты представлены в таблице ниже.

Таблица 12. Меры защиты

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

		– обеспечивать целостность данных; – производить обнаружений вторжений.
--	--	--

В ИСПДн введены следующие организационные меры защиты:

- в Учреждении осуществляется контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания;
- ведется учет носителей информации;
- носители информации хранятся в сейфе;
- в Учреждении существует отдел/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 так же 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.

3.7 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;
- назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;
- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же 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.