Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий и телекоммуникаций
Кафедра организации и технологии защиты информации

Утверждена распоряжением по институту
от «12» марта 2020 г. № 029-р/12.00
Выполнена по заявке организации
(предприятия)_____
_____

Допущена к защите
«18» июня 2020 г.
Зав. кафедрой организации и технологии защиты информации
канд. техн. наук, доцент
В. И. Петренко

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ОПЕРАТОРУ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ПОСТРОЕНИЮ СИСТЕМЫ ЗАЩИТЫ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРЕДПРИЯТИЯ

Рецензенты:
Герасимов Владимир Павлович
канд. техн. наук, доцент, доцент кафедры информационных систем ФГБОУ ВО «Ставропольский государственный аграрный университет»

Нормоконтролер:
Бисюков Виктор Михайлович
доцент, доцент кафедры организации и технологии защиты информации
_____
подпись)

Дата защиты «01» июля 2020 г.

Оценка _____

Выполнил (а):
Шахбазян Владислав Виленович
студент 4 курса, группы ИНБ-б-о-16-2 направления подготовки 10.03.01 «Информационная безопасность» профиль «Организация и технология защиты информации» очной формы обучения
_____
подпись)

Руководитель:
Бисюков Виктор Михайлович
доцент, доцент кафедры организации и технологии защиты информации
_____
подпись)

Ставрополь, 2020 г.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АРМ – автоматизированное рабочее место
АС – автоматизированная система
ЗПДн – защита ПДн
ИБ – информационная безопасность
ИСПДн – информационная система ПДн
КЗ – контролируемая зона
ЛВС – локально–вычислительная сеть
НМД – нормативно–методические документы
НДВ – не декларированные возможности
ПДн – персональные данные
ПО – программное обеспечение
ППО – прикладное программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
СВТ – средства вычислительной техники
СЗИ – средство защиты информации
СЗПДн – система защиты ПДн
СКЗИ – средства криптографической защиты информации
СП - структурные подразделения
СПО – системное программное обеспечение
ССОП – сети связи общего пользования
СУБД – система управления базами данных
СФХ – структурно–функциональные характеристики
ТЗ – техническое задание
ТСр – технические средства
УЗ – уровень защищенности
УБПНд – угрозы безопасности ПДн
ФСБ – Федеральная служба безопасности
ФСТЭК – Федеральная служба по техническому и экспортному контролю
ЦСМ – Центр стандартизации, метрологии и сертификации

ВВЕДЕНИЕ

Современные информационные системы предприятий и организаций, наряду с хранением и обработкой деловой информации, решают задачи хранения и обработки ПДн сотрудников и контрагентов. Это влечет за собой необходимость организации обработки и защиты ПДн в соответствии с требованиями действующего законодательства в данной области.

Защита ПДн является одной из важнейших задач системы обеспечения информационной безопасности в организации любого масштаба и любой организационно–правовой формы хозяйствования [1].

Актуальность работы обусловлена тем, что оператор обязан выполнять требования ФЗ №152 «О персональных данных», но при организации защиты ПДн в ИСПд он сталкивается с трудностями по учету требований большого количества нормативных документов, регламентирующих процесс построения СЗПДн.

Целью работы является повышение уровня информационной безопасности предприятия за счёт минимизации расходов и повышения эффективности, при построении СЗ в ИСПДн.

Задачи для достижения поставленной цели:

– анализ требований НМД, регламентирующих порядок построения СЗПДн в ИСПДн,

– разработка рекомендаций оператору ПДн по построению СЗПДн в ИСПДн с учётом требований НМД,

– апробация предложенных рекомендаций по построению СЗПДн в ИСПДн реальной организации,

– оценка эффективности предложенных рекомендаций и технико-экономическое обоснование возможности их реализации в СЗПДн ИСПДн организации.

Объектом исследования является ИСПДн.

Предметом исследования является технология построения СЗПДн в ИСПДн

1 Разработка рекомендаций оператору персональных данных по построению системы защиты в информационной системе персональных данных

1.1 Анализ требований нормативно-методических документов, регламентирующих порядок построения системы защиты в информационной системе персональных данных

Перечень основных документов, регламентирующих порядок построения СЗПДн в ИСПДн представлен в приложении А.

Анализ документов позволяет сделать вывод о том, что при организации работ по построению СЗПДн и ИСПДн оператор сталкивается с трудностями по полному учёту требований данных документов, т. е. необходима стройная методика, позволяющая выполнить эту работу с наибольшей эффективностью.

Кроме того, на предприятии должны быть отработаны локальные нормативные акты по организации защиты ПДн в ИСПДн.

Результаты анализа требований основных НМД в области построения СЗПДн для ИСПДн представлен в таблице 1.

Таблица 1 – Анализ нормативно–методической базы, регламентирующей порядок разработки СЗПДн в ИСПДн

Нормативный документ	Требования документа	Результат
ФЗ 152 «О ПДн »	– назначение ответственного за обработку ПДн, – издание оператором ОРД, определяющих политику оператора в отношении обработки ПДн, – применение правовых, организационных и технических мер по защите ПДн, – применение сертифицированных СрЗИ, – учет машинных носителей ПДн, – обнаружение фактов НСД к ПДн и принятием мер, – контроль за принимаемыми мерами по обеспечению безопасности ПДн	– перечень ПДн, подлежащих защите в ИСПДН, – политика оператора в отношении обработки ПДн, – требования к ФСТЭК и ФСБ по методическому сопровождению ФЗ №152, – требования к набору ОРД при построении СЗПДн в ИСПДН
ПП от 01.11. 2012. N 1119	– уровни защищенности ПДн при их обработке в ИС ПДн,	– уровни защищённости ПДн в ИСПДН,

Нормативный документ	Требования документа	Результат
	– требования к защите ПДн в ИСПДн, в соответствии с ровни защищенности ПДн	– типы угроз, – требования к защите ПДн
ПП РФ от 06.06.2008 № 512	Требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне информационных систем ПДн утверждены постановлением.	порядок работы с носителями биометрических ПДн
ПП РФ от 15 сентября 2008 г. № 687	Положение об особенностях обработки ПДн, осуществляемой без использования средств автоматизации.	Порядок обработки ПДн без средств автоматизации
ПП РФ №211 от 21 марта 2012г	– назначение ответственного за обработку ПДн, – определен перечень ОРД по ПДн, – требование по обезличиванию ПДн в ИСПДН	Перечень ОРД описывающих правила работы с обезличенными ПДн
Приказ №17 ФСТЭК	требования к обеспечению ЗИ от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию	– модель угроз безопасности информации, – ТЗ на создание СЗИ, – ОРД по ЗИ, – анализ уязвимостей ИС.
Приказ № 21 ФСТЭК	– состав организационных и технических мер по защите ПДн, при их обработке в ИСПДН, – определяет порядок выбора организационных и технических мер по обеспечению безопасности ПДн, подлежащих реализации в ИС в рамках СЗПДн.	–состав организационных и технических мер по защите ПДн в ИСПДН, – требования к сертифицированным СрЗИ.
МД ФСТЭК «Базовая модель угроз для ПДн в ИСПДН»	Методика построения модели угроз для ПДн в ИСПДН	Перечень потенциальных угроз безопасности ПДн, при их обработке в ИСПДН
МД «Методика определения актуальных угроз безопасности ПДн, при их обработке в ИСПДН»	Методика определения актуальных угроз безопасности ПДн, при их обработке в ИСПДН	Перечень актуальных угроз безопасности ПДн, при их обработке в ИСПДН и вероятности их реализации
Приказ ФСБ России от 10 июля 2014 г. N 378	– состав и содержания организационных и технических мер по защите ПДн при их обработке в ИСПДН с использованием СКЗИ, необходимых для выполнения установленных Правительством РФ требований к защите ПДн для каждого из уровней защищенности»	Реализация криптографической защиты информации

Нормативный документ	Требования документа	Результат
Приказ ФСБ России от 9 февраля 2005 года № 66.	Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных средств защиты информации.	
ГОСТ 34.601–90.	Определяет этапы и содержание этапов работ по разработке АС	– ЧТЗ на выполнение работ по созданию СЗПд в ИСПд, – эксплуатационная и ОРД для ИСПДН

1.2 Разработка рекомендаций оператору персональных данных по построению системы защиты в информационной системе персональных данных

Создание СЗПДн – это комплекс мер технического и организационного характера, направленных на защиту сведений, отнесенных в соответствии с ФЗ от 27.06.2006 N 152 к ПДн.

В соответствии с заданием, и с учётом требований нормативных документов по ЗПДн, разработаны рекомендации оператору ПДн по построению СЗПДн в ИСПДн.

Последовательность работы оператора по реализации предложенных рекомендаций представлен в таблице 2.

Таблица 2 – Последовательность работы оператора ПДн по построению СЗПДн в ИСПДн

Этапы работы	Содержание работы	Разрабатываемые документы
Разработка перечня ПДн обрабатываемых в ИСПДн	– цели обработки ПДн – категории ПДн, – правовое обоснование обработки ПДн	Перечень ПДн в ИСПДн
Определение УЗ ПДн	– категории ПДн, тип угроз, объём ПДн	Акт по УЗ ИСПДн
Выбор базового набор мер для определённого УЗ ПДн	– анализ прил. 2 к Пр ФСТЭК №21	Перечень базового набора мер
Адаптация базового набора мер	– цели и задачи ИСПДн, анализ СФХ, – применяемые технологии в ИСПДн	Перечень адаптированного набора мер

Этапы работы	Содержание работы	Разрабатываемые документы
Уточнение адаптированного базового набора мер	– модель нарушителя, анализ уязвимостей, – перечень актуальных угроз	Модель угроз
Выбор перечня организационных и технических мер защиты ПДн для ИСПДн	– выбор перечня мер в соответствии с перечнем угроз и возможностей нарушителя	Перечень организационных и технических мер
Выбор ТСр для СЗПДн в соответствии с выбранным УЗ	– выбор ТСр с учётом УЗ и класса защиты ИС	Перечень сертифицированных ТСр
Оценка эффективности СЗПДн и технико -экономическое обоснование возможности реализации СЗПДн	– оценка эффективности по критерию величины риска ИБ для ИСПДн	Результаты расчётов

В данной работе представлены рекомендации оператору по реализации каждого из этапов работы по построению СЗПДн в ИСПДн.

1.2.1 Порядок разработки перечня персональных данных

Перечень ПДн является правовой основой построения системы защиты Пд в ИС организации. Перечень ПДн оформляется отдельным разделом в перечне сведений, составляющих конфиденциальную информацию организации.

Разработкой перечня должна заниматься постоянно действующая экспертная комиссии.

Результаты работы оформляются перечнем ПДн, составляющих коммерческую тайну, который имеет следующие графы (таблица 3).

Таблица 3 – Перечень ПДн предприятия

№ п/п	Категории персональных данных	Цель обработки персональных данных	Категории субъектов, персональные данные которых обрабатываются	Правовое основание обработки персональных данных

Перечень подписывается всеми членами экспертной комиссии и утверждается первым руководителем предприятия.

1.2.2 Порядок определения требуемого уровня защищённости персональных данных

Требуемый уровень защищённости ИСПДн определяется с учётом требований ПП 1119.

Под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн, при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия.

Угрозы 1 - го типа актуальны для ИСПДн где актуальны угрозы наличия НДВ в системном ПО.

Угрозы 2 - го типа актуальны для ИСПДн где актуальны угрозы наличия НДВ в прикладном ПО.

Угрозы 3 - го типа актуальны для ИСПДн, где актуальны угрозы, не связанные с НДВ в системном и прикладном ПО.

Выбор уровня защищённости ПДн производится с учётом требований постановления правительства № 1119 по таблице 4.

Таблица 4 – Выбор уровня защищённости ПДн

Категория Пд	Кол–во/субъекты ПДн	Тип угроз		
		1 го типа	2 го типа	3 го типа
Биометрические	Любые	УЗ 1	УЗ 2	УЗ 3
Специальные	> 100 000	УЗ 1	УЗ 1	УЗ 2
	< 100 000 (или СО)	УЗ 1	УЗ 2	УЗ 3
Иные категории ПДн	> 100 000	УЗ 1	УЗ 2	УЗ 3
	< 100 000 (или СО)	УЗ 1	УЗ 3	УЗ 4
Общедоступные	> 100 000	УЗ 2	УЗ 2	УЗ 4
	< 100 000 (или СО)	УЗ 2	УЗ 3	УЗ 4

1.2.3 Порядок определение базового набора мер

Мера защиты ПДн, это определённое требование (правило, норма) к защите ПДн, которая должна быть выполнена, при организации защиты ПДн.

Базовый набор мер определяется на основе определённого уровня защищённости ИСПд, с учётом требований приказа ФСТЭК №21 [8].

1.2.4 Порядок адаптации базового набора мер

Адаптация базового набора мер предполагает исключение мер, непосредственно связанных с информационными технологиями, не применяемыми в исследуемой ИСПДн, или СФХ, не свойственными данной ИС. Анализ применяемых технологий, ПО и СФХ ИСПДн предлагается проводить по следующим характеристикам (таблицы 5-8).

Таблица 5 – Анализируемые СФХ ИСПДн

Анализируемые СФК ИСПДн	Возможные варианты анализируемых характеристик
По структуре ИС	автономное автоматизированное рабочее место
	локальная ИС
	распределенная ИС
По используемым информационным технологиям	системы на основе виртуализации
	системы, реализующие «облачные вычисления»
	системы с мобильными устройствами
	системы с технологиями беспроводного доступа
	грид–системы
	суперкомпьютерные системы
По свойствам архитектуры	системы на основе «тонкого клиента»,
	системы на основе одноранговой сети,
	файл–серверные системы
	центры обработки данных
	системы с удаленным доступом пользователей,
	использование разных типов операционных систем
	использование прикладных программ, независимых от операционных систем,
	использование выделенных каналов связи
По наличию взаимосвязей с иными ИС	взаимодействующая с системами
	невзаимодействующая с системами
По наличию подключений к сетям связи общего пользования	подключенная,
	подключенная через выделенную инфраструктуру (gov.ru или иную),
	неподключенная
По размещению технических средств	расположенные в пределах одной контролируемой зоны
	расположенные в пределах нескольких контролируемых

Анализируемые СФК ИСПДн	Возможные варианты анализируемых характеристик
	зон,
	расположенные вне КЗ
По режимам обработки информации в ИС	многопользовательский
	однопользовательский
По режимам разграничения прав доступа	без разграничения
	с разграничением
По режимам разделения функций по управлению ИС	без разделения
	выделение рабочих мест для администрирования в отдельный домен
	использование различных сетевых адресов,
	использование выделенных каналов для администрирования
По подходам к сегментированию ИС	без сегментирования,
	с сегментированием

По предложенным характеристикам анализируется ИСПДн организации.

Таблица 6 – Названия и версии основного системного и прикладного ПО используемого в ИСПДн

№ п.п.	Название и версия ПО	Назначение ПО	Места установки ПО	Тип ПО (системное или прикладное)
1.				
2.				

Таблица 7 – Сведения об основных информационных технологиях, используемых в ИСПДн

№ п.п.	Название информационной технологии	Использование
1.		
2.		

Таблица 8 – Межсетевые взаимодействия ИС

№ п.п.	Сеть, с которой осуществляется взаимодействие	Характер и особенности взаимодействия	Участники взаимодействия в ЛВС
1.			
2.			

По предложенным характеристикам анализируется ИСПДн организации. Результаты анализа оформляются актом.

1.2.5 Порядок уточнения адаптированного базового набора организационных и технических мер

Уточнение базового адаптированного набора мер производится в следующей последовательности:

– построение базовой модели угроз для ИСПДн и определение на её основе актуальных угроз безопасности ИСПДн [7],

– уточнение адаптированного базового набора мер защиты ПДн.

Базовая модель угроз в своём составе должна содержать:

– описание возможностей нарушителей (модель нарушителя),

– возможных уязвимостей информационной системы,

Модель нарушителя содержит:

– вид и тип и возможности актуального нарушителя (таблица 9),

– предположения об имеющейся у нарушителя информации (таблица 10),

– предположения об имеющихся у нарушителей средствах атак (таблица 11).

Таблица 9 – Определение вида и типа нарушителей

№ п/п	Вид нарушителя	Тип нарушителя	Функциональная характеристика нарушителя
1.	Внешний	Тип 1	отдельные лица, ведущие злоумышленную деятельность, не имеющие доступа в КЗ.
2.	Внутренний	Тип 2	- посетители, имеющий разовый доступ в КЗ, - определенные категории обсуживающего персонала и представителей ремонтных организаций, не имеющих доступ к компонентам узлов,
		Тип 3	представители технических и обслуживающих служб, консультационных и других вспомогательных служб, находящихся в пределах КЗ на постоянной основе или периодически
		Тип 4	сотрудники предприятия, не являющиеся операторами или администраторами ИСПДн
		Тип 5	сотрудник, являющийся оператором АРМ ИСПДн
		Тип 6	администраторы ИСПДн.
		Тип 7	сотрудники организаций, осуществляющих обслуживание узлов на постоянной основе в соответствии с заключенными договорами

Таблица 10 – Предположения об имеющейся у нарушителя информации

№ п/п	Возможные виды потенциально опасной информации	Имеющаяся у нарушителя информация
1.	Сведения о парольной и аутентифицирующей информации системы	Не обладает. При этом предполагается, что внутренний нарушитель обладает, в пределах своих полномочий, сведениями о собственной аутентифицирующей информации
2.	Планы зданий, мест размещения технических средств с привязкой к конкретным помещениям	Обладает частично
3.	Данные о составе пользователей	Достоверной информацией не обладает
4.	Сведения об информационных ресурсах узлов – порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков	Достоверной информацией не обладает
5.	Данные об организации работы, структуре и используемых технических, программных и программно–технических средствах узлов	Только имеющиеся в свободном доступе (например, сети Интернет)
6.	Все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно–техническими мерами	Достоверной информацией не обладает
7.	Долговременные ключи криптосредств	Не обладает
8.	Данные об уязвимостях СПО и ППО	Только описания, имеющиеся в свободном доступе
9.	Сведения о возможных для данного узла каналах атак	Достоверной информацией не обладает
10.	Информация о способах (методах) атак	Только описания, имеющиеся в свободном доступе (например, сети Интернет, печатных изданиях)
11.	Данные об организациях осуществляющих поставку, ремонт, пуско–наладочные и монтажные работы, обслуживание технических и программных средств	Только сведения, имеющиеся в свободном доступе (например, сети Интернет)
12.	Данные о местах ремонта и обслуживания технических средств узлов	Только сведения, имеющиеся в свободном доступе (например, сети Интернет)
13.	Общая информированность нарушителя	Нарушитель 1 типа не обладает достоверной информацией об объекте и порядке обработки информации, информацию получает из источников свободного доступа.

№ п/п	Возможные виды потенциально опасной информации	Имеющаяся у нарушителя информация
		Нарушители 2, 3, 4 типов обладают определенной информацией о структуре объектов, однако не имеют достоверной информации об особенностях обработки информации и об используемых сетях связи, работающих на едином ключе. Нарушитель 5 типа имеет представление об особенностях обработки информации на объектах, однако не имеет достоверной информации и не имеет сведений об используемых сетях связи, работающих на едином ключе.

Таблица 11 – Предположения об имеющихся у нарушителей средствах атак

№ п/п	Возможные средства атак	Имеющиеся у нарушителя средства атак
1.	Аппаратные компоненты криптографических средств	Отсутствует
2.	Доступные в свободной продаже технические средства и программное обеспечение	Возможно применение подобных средств (включая общедоступные компьютерные вирусы)
3.	Специально разработанные технические средства и программное обеспечение	Отсутствует
4.	Штатные средства	Штатные средства размещены в пределах КЗ
5.	Распределенные ресурсы различных сетей, в том числе сети Интернет	Возможно организация распределенных атак

Актуальные угрозы для ИСПДн определяются по методическим документам ФСТЭК «Базовая модель угроз» и «Методика определения актуальных угроз» [5,6].

На первом этапе определяется исходный уровень защищённости ИСПДн Y_1 (таблица 12) [8].

Таблица 12 – Порядок определения исходного уровня защищённости ИСПДн

Технические и эксплуатационные характеристики ИСПДН организации		Уровень защищенности		
Типы характеристик	Характеристики ИСПДн	Высокий	Средний	Низкий
По территориальному размещению	локальная ИСПДн, развернутая в пределах одного здания		–	–

Технические и эксплуатационные характеристики ИСПДН организации		Уровень защищенности		
Типы характеристик	Характеристики ИСПДн	Высокий	Средний	Низкий
По наличию соединения с сетями общего пользования	ИСПДн, имеющая одноточечный вход в сеть общего пользования	–	–	
По встроенным (легальным) операциям с записями баз ПДн	чтение, поиск, передача		–	–
По разграничению доступа к персональным данным	ИСПДн, к которой имеет доступ определенный перечень работников либо субъект ПДн	–	–	
По наличию соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая предприятию			
По уровню обобщения (обезличивания) ПДн	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	–		–
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн	–		–

ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий», а остальные – среднему уровню защищенности (Y1= 0).

ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний», а остальные – низкому уровню защищенности (Y1= 5).

ИСПДн имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2 (Y1= 10).

На следующем этапе определяется перечень актуальных угроз с учётом методический рекомендаций ФСТЭК [8]. Результаты работы отражаются в сводной таблице 13.

Таблица 13 – Результаты работы по определению актуальных угроз для ИСПДн

Тип угроз безопасности ПДн	Коэффициент вероятности	Вероятность возникновения угрозы	Коэффициент реализуемости угрозы	Возможность реализации угрозы	Опасность угрозы	Актуальность угрозы
	Угрозы утечки по техническим каналам					
	Угрозы НСД					

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$),
- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры затрудняют ее реализацию ($Y_2 = 2$),
- средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры недостаточны ($Y_2 = 5$),
- высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты ($Y_2 = 10$).

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20.

По значению коэффициента Y определяется возможность реализации угрозы по следующим диапазонам:

0,3 – низкая,

0,6 – средняя,

0,8 – высокая,

0,8 – очень высокая.

Оценка опасности угрозы определяется на основе опроса специалистов по вербальным показателям опасности с тремя значениями:

- *низкая опасность* – если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн,
- *средняя опасность* – если реализация угрозы может привести к негативным последствиям для субъектов ПДн,
- *высокая опасность* – если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

Дале по таблице 14 определяется актуальность каждой угрозы.

Таблица 14 – Порядок определения актуальных угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Полученные результаты учитываются при проведении уточнения адаптированного базового набора мер, т.е. из перечня мер исключаются меры, не соответствующие актуальным угрозам и возможностям актуального нарушителя.

В дальнейшем каждой актуальной угрозе сопоставляется техническая и организационная мера из набора базовых мер для соответствующего уровня защищённости ПДн. [8]

1.2.6 Порядок выбора организационных и технических мер

По таблице 15 определяется соответствие актуальной угрозы организационным и техническим мерам из набора адаптированный мер.

Таблица 15 – Соответствие угроз организационным и техническим мерам из набора адаптированный мер

№ п/п	Угрозы безопасности ПДн	Номер и условное обозначение организационных и технических мер
1	Угрозы утечки информации по техническим каналам	
1.1	перехват передаваемой по техническим каналам информации	ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователей в информационной системе
1.2	визуальный просмотр на экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн	ИАФ.2 Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации
1.3	Угрозы утечки по техническим каналам	АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа полномочий пользователей в информационной системе.
2.	Угрозы НСД в ИСПДн	
2.1	Угрозы нарушения процессов идентификации и аутентификации субъектов и объектов доступа	ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешние пользователи)
2.2	Угрозы нарушения доступа субъектов доступа к объектам доступа:	УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе и внешних пользователей
2.3	Угрозы использования уязвимостей ИСПДн:	АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей; АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения и средств защиты информации
2.4	Угрозы непосредственного доступа в операционную среду ИСПДн:	УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации; УПД.17 Обеспечение доверенной загрузки средств вычислительной техники

2.5	Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:	ЗИС.17 Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
2.6	Угрозы программно-математических воздействий:	АВЗ.1 Реализация антивирусной защиты; АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов) ЗСВ.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре
2.7	Угрозы несанкционированного физического доступа к ТС и системам обеспечения:	ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены
2.8	Угрозы несанкционированного физического доступа к ТС и системам обеспечения	ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены
2.9	Угрозы неправомерных действий со стороны лиц, имеющих право доступа к информации	ЗНИ.5 Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных ЗНИ.1 Учет машинных носителей персональных данных УПД.15 Регламентация и контроль использования в информационной системе мобильных технических средств
2.10	Угрозы нарушения организации работы подсистем регистрации событий безопасности	ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации ЗСВ.5 Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией
2.11	Угрозы средствам виртуализации	ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации ЗСВ.5 Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией

1.2.7 Порядок выбора технических средств для реализации предложенных технических мер защиты

Затем для реализации технических мер выбирается перечень технических средств (таблица 16) с учётом класса защиты (таблица (17).

Таблица 16 – Соответствие технических средств защиты техническим мерам

№ п.п	Мера	Техническое средство
1.	Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	Aladdin SAM, АПКШ Континент, ПАК VipNet, TrustAccess, Imperva SecureSphere, Встроенные средства ОС и ППО
2.	Управление доступом субъектов доступа к объектам доступа (УПД)	СЗИ от НСД SecretNet, ПАК Соболь, Oracle IAMS, АПКШ Континент, ПАК VipNet, TrustAccess, Imperva SecureSphere, Встроенные средства ОС и ППО
3.	Ограничение программной среды (ОПС)	СЗИ от НСД SecretNet, Код безопасности: Инвентаризаци
4.	Защита машинных носителей информации (ЗНИ)	СЗИ от НСД SecretNet
5.	Регистрация событий безопасности (РСБ)	HP ArcSight, McAfee SIEM, Встроенные механизмы СЗИ
6.	Антивирусная защита (АВЗ)	Антивирус Касперского, McAfee Antivirus, Security Studio, Endpoint Protection, TrendMicro Deep Security
7.	Обнаружение (предотвращение) вторжений (СОВ)	Детектор атак «Континент», Palo Alto, StoneGate, CheckPoint, Imperva SecureSphere, Антивирусные средства с функциями СОВ
8.	Контроль (анализ) защищенности ПДн(АНЗ)	MaxPatrol / xSpider, Комплексный аудит ИС, Тест на проникновение
9.	Обеспечение целостности информационной системы и ПДн(ОЦЛ)	СЗИ от НСД SecretNet, ПАК Соболь, Средства резервного копирования
10.	Обеспечение доступности ПДн(ОДТ)	Отказоустойчивые конфигурации Средства резервного копирования
11.	Защита среды виртуализации (ЗСВ)	vGate, TrendMicro Deep Security, Сертифицированная VMware vSphere 5.1
12.	Защита технических средств (ЗТС)	Применяемые на объекте системы физической охраны (видеонаблюдение, контроль и управление доступом, сигнализация и пр).
13.	Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	СЗИ от НСД SecretNet, vGate, АПКШ Континент, Arbor
14.	Выявление инцидентов и реагирование на них (ИНЦ)	Ведение журнала инцидентов
15.	Управление конфигурацией информационной системы и СЗПДн (УКФ)	АПКШ Континент

Таблица 17 – Порядок выбора технических средств защиты в составе ИСПДн с учетом требований к их классу защиты

Уровень защищённости ПДн	Класс защиты									Уровень контроля ПО на отсутствие НДВ
	СВТ	САВЗ		СОВ		МЭ		СДЗ		
		Угрозы 2	Угрозы 3 типа	Угрозы 2 типа	Угрозы 3 типа	Угрозы 1 или 2 типа	Угрозы 3 типа	Угрозы 1 или 2 типа	Угрозы 3 типа	
УЗ1	≥ 5 кл	≥4кл		≥4кл		≥3кл	≥4кл	≥4кл		4 уровень
УЗ2	≥5 кл	≥4кл		≥4кл		≥3кл	≥4кл	≥4кл		4 уровень
УЗ3	≥5кл	≥4кл	≥5кл	≥4кл	≥5кл	≥4кл	≥5кл	≥4кл	≥5кл	4 уровень в случае угроз 2 типа
УЗ4	≥6кл	≥5кл		≥5кл		≥5кл		≥5кл		Требований нет

Затем выбранные к реализации организационные и технические меры, а также средства защиты учитываются при разработке технического задания на разработку СЗПДн в ИСПДн.

1.3 Порядок оценки эффективности системы защиты в информационной системе персональных данных

Оценку эффективности СЗПДн в ИСПДн организации предлагается проводить по критерию количественной оценки риска ИБ для ИСПДн [8].

Этапы оценки риска ИБ представлены в таблице 18.

Таблица 18 – Этапы оценки риска ИБ ИСПДн

Этапы	Название этапов
Этап 1	Определение риска несоответствия требованиям законодательства в области ЗПДн в ИСПДн
Этап 2	Определение вероятностей реализации хотя бы одной из актуальных угроз
Этап 3	Определение степени использования организационных и технических средств защиты ИС
Этап 4	Определение количественного значения риска информационной безопасности

Числовое значение величины риска ИБ определяется по формуле 1 [19].

$$R = \text{Ругр} \cdot Rn \cdot C \frac{\text{Ko}+\text{K}t}{2} \cdot 100\%,. \quad (1)$$

где R – численная величина риска реализации угроз ИБ,

Ругр – вероятность реализации хотя бы одной угрозы из всего перечня угроз,

Rn – риск несоответствия требованиям законодательства,

C – ценность актива, определяется как отношение стоимости ПДн, обрабатываемых в ИСПДн к стоимости всего предприятия (0…1),

Ko – вероятность использования организационных уязвимостей,

Kt – вероятность использования технических уязвимостей.

Ели значение риска ИБ меньше 5 % то уровень защиты ПД и ИСПДн признаётся достаточным.

1.4 Выводы по разделу

В качестве основных выводов по разделу можно отметить:

– на основании анализа требований НМД, регламентирующих порядок построения СЗПДн в ИСПДн, разработаны рекомендации оператору ПДн по построению СЗПДн в ИСПДн предприятия,

– предложена последовательность действий оператора:

1) разработка перечня ПДн обрабатываемого в ИСПДн,
2) определение уровня защищённости ИСПДн,
3) выбор базового набор мер для определённого УЗ ИСПДн,
4) адаптация базового набора мер,
5) уточнение адаптированного базового набора мер,
6) определение перечня организационных и технических мер защиты ПДн для ИСПДн,
7) выбор технических средств для реализации предложенных технических мер ЗПДн в соответствии с выбранным УЗ,

– предложена методика оценки эффективности СЗПДн в ИСПДн по критерию количественного значения величины риска ИБ для ИСПДн.

2 Построение системы защиты персональных данных в информационной системе персональных данных ФБУ «ЦСМ»

В соответствии с заданием и в целях апробации предложенных рекомендаций, проведём построение СЗПДн в ИСПДн ФБУ «ЦСМ».

2.1 Анализ ФБУ «ЦСМ», как оператора персональных данных. Разработка перечня защищаемых персональных данных

Штатная структура ЦСМС представлена на рисунке 1.

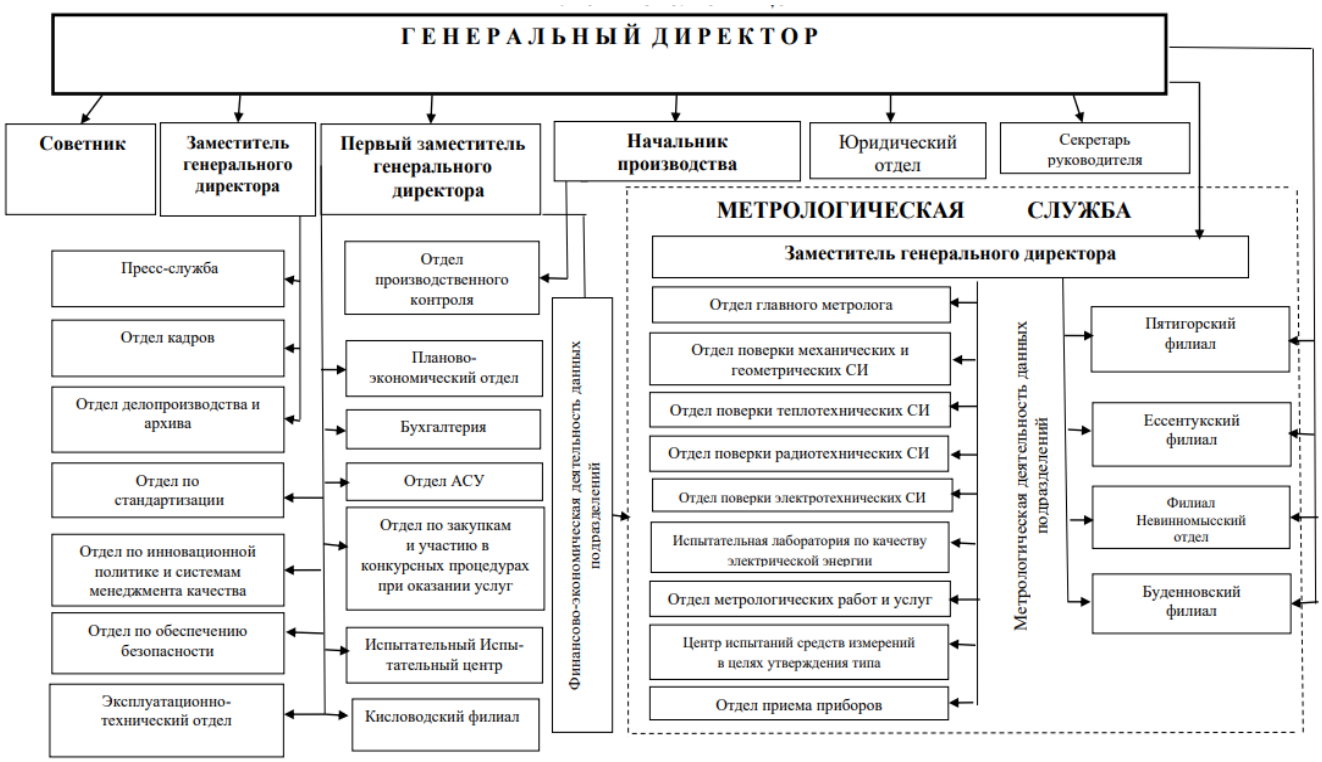

Рисунок 1 – Штатная структура ФБУ «ЦСМ»

Основные направления деятельности организации представлены на рисунке 2.

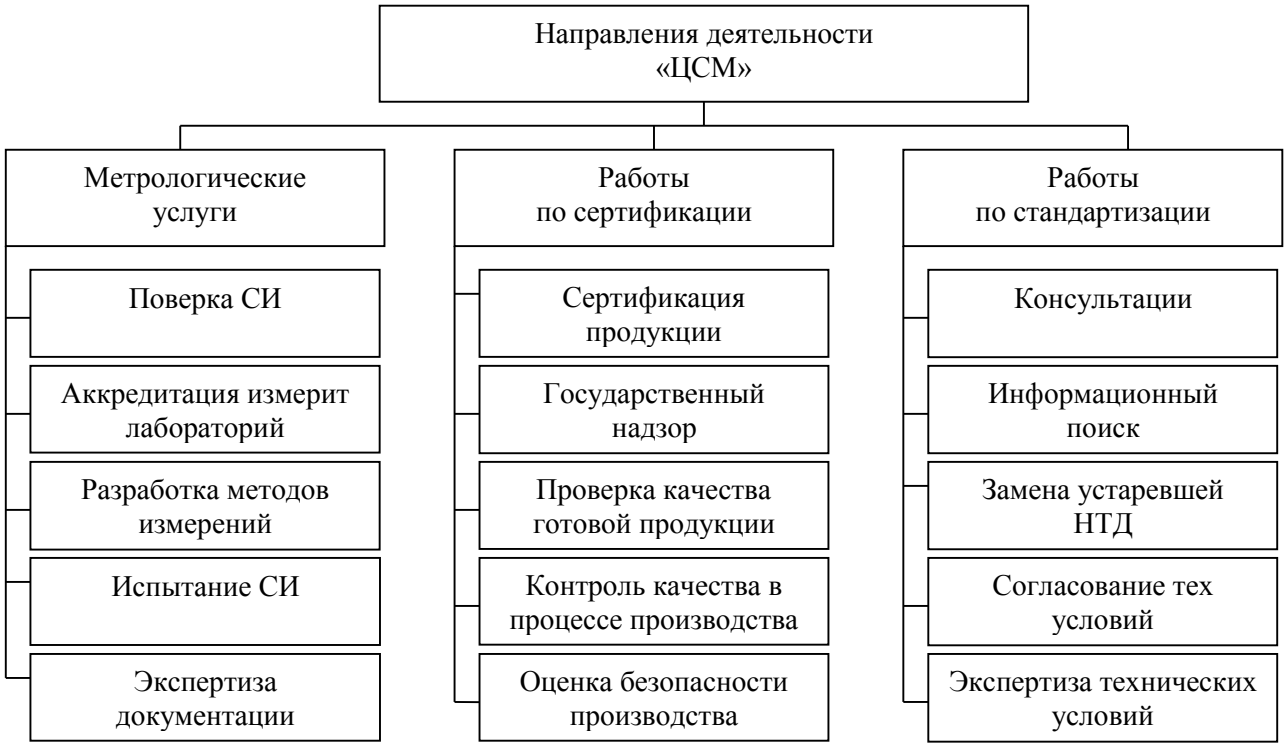

Рисунок 2 – Направления деятельности ЦСМ

Технологическая схема обработки ПДн в организации представлена на рисунке 3.

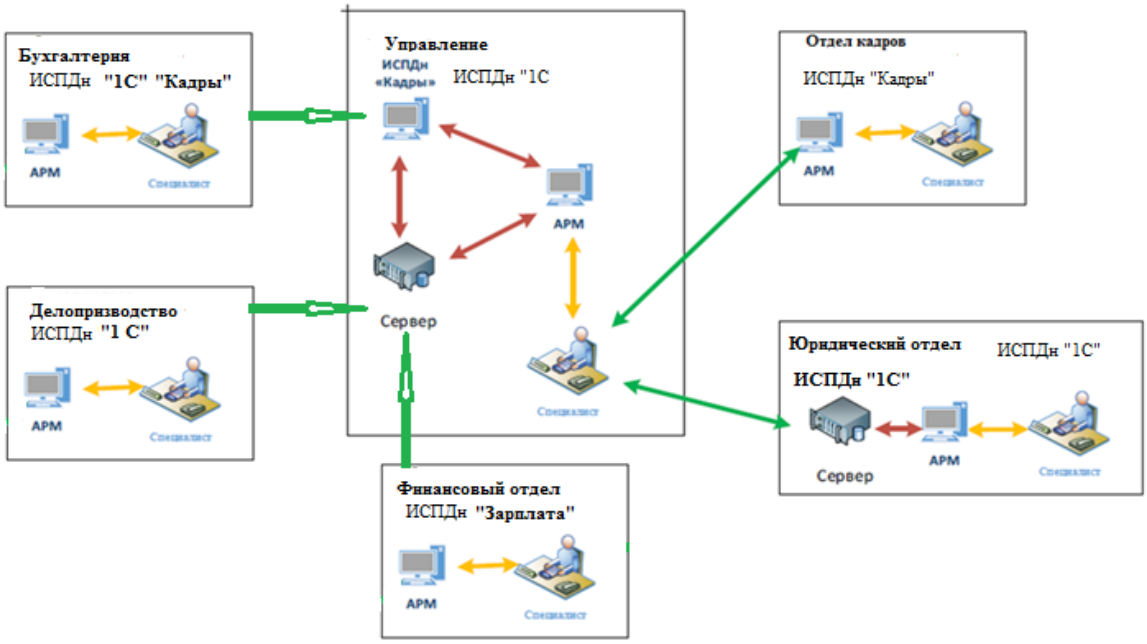

Рисунок 3 - Технологическая схема обработки ПДн в ФБУ «ЦСМ»

В организации обрабатываются ПДн следующих категорий субъектов:

– кандидатов, работников, родственников работников, лиц, ранее состоявших в трудовых отношениях с ФБУ «ЦСМ»,

– физических лиц по договорам гражданско-правового характера,

– контрагентов – физических лиц, представителей и работников контрагентов (юридических лиц).

При приеме на работу в ФБУ «ЦСМ» работник отдела кадров обрабатывает следующие анкетные и биографические данные работника:

– общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, состав семьи, паспортные данные, адрес места жительства и др.),

– сведения о воинском учете,

– другие данные, необходимые при приеме на работу в соответствии с требованиями трудового законодательства.

В дальнейшем в личную карточку работника по форме Т-2 вносят сведения:

– о переводах на другую работу,

– аттестации, повышении квалификации, профессиональной переподготовке,

– наградах (поощрениях), почетных званиях,

– социальных льготах, на которые работник имеет право в соответствии с законодательством.

Цели обработки персональных данных работников ФБУ «ЦСМ»:

– ведение кадрового учета,

– учет рабочего времени работников,

– расчет заработной платы работников,

– ведение налогового учета,

– ведение воинского учета,

– предоставление в государственные органы регламентированной отчетности,

– обязательное и добровольное медицинское страхование работников,

– бронирование и оплата билетов и гостиничных номеров работникам,

– архивное хранение данных,

– содействие работнику в трудоустройстве, обучении, продвижении по службе, использовании различных льгот.

Во исполнение требований ФЗ 152 в организации имеются следующие организационно-распорядительные документы, регламентирующие обработку ПДн:

– Политика обработки ПДн в ФБУ «ЦСМ»,

– Положение о защите ПДн работников ФБУ «ЦСМ»

Разработанный перечень ПДн организации представлен в приложении Б.

2.2 Определение требуемого уровня защищённости персональных данных в ФБУ «ЦСМ»

Требуемый уровень защищённости ИСПДн определялся с учётом рекомендаций первого раздела.

Выбор уровня защищённости производится с учётом таблицы 14.

Таблица 14 – Выбор уровня защищённости ПДн

Категория Пд	Кол–во/субъекты ПДн	Тип угроз		
		1 го типа	2 го типа	3 го типа
	< 100 000 (или СО)	УЗ 1	УЗ 2	УЗ 3
Иные категории ПДн	< 100 000 (или СО)	УЗ 1	УЗ 3	УЗ 4
	< 100 000 (или СО)	УЗ 2	УЗ 3	УЗ 4

Итоговый уровень защищенности ИСПДн ФБУ «ЦСМ» представлен в таблице 15.

Таблица 15 – Итоговый уровень защищенности ИСПДн ФБУ «ЦСМ»

№ п/п	Наименование ИСПДН	Категория ПДн	Тип угроз	Объем ПДн	Уровень защищенности ИСПДН
1.	«1С»	Иные	2–й тип	< 100 000 (или СО)	УЗ 3
2.	«Кадры»	Иные	2–й тип	< 100 000 (или СО)	УЗ 3

№ п/п	Наименование ИСПДН	Категория ПДн	Тип угроз	Объем ПДн	Уровень защищенности ИСПДН
3.	«Зарплата»	Иные	2–й тип	< 100 000 (или СО)	УЗ 3

Общая характеристика ИСПДн предприятия и уровни защищенности ИСПДН, представлены в таблице 16.

Таблица 16 – Общая характеристика ИСПДн предприятия и уровни защищенности ИСПДн

№ п/п	Название ИСПДн	Структура ИСПДн	Подключения к ССОП	Режим обработки ПДн	По разграничению прав доступа к ПДн	Местонахождение ТС относительно границ РФ	Объем обрабатываемых ПДн	Категория обрабатываемых ПДн	Уровень защищенности
1.	«1С»	Локальная	Есть	МП	С РПД	В пределах РФ	< 100 000 (или СО)	Иные	УЗ 3
2.	«Кадры»	Локальная	Есть	ОП	С РПД	В пределах РФ	< 100 000 (или СО)	Иные	УЗ 3
3.	«Зарплата»	Локальная	Есть	МП	С РПД	В пределах РФ	< 100 000 (или СО)	Иные	УЗ 3

Таким образом, для ИСПд ФБУ «ЦСМ» определён 3 уровень защищённости для всех 3- х ИСПДн организации.

Выбор базового набора мер для ФГБУ «ЦСМ»

Базовый набор мер для 3-го уровня защищённости представлен в приложении В [4].

Адаптация базового набора мер по обеспечению безопасности персональных данных

Адаптация базового набора мер по обеспечению безопасности ПДн проводится с учетом структурно–функциональных характеристик, информационных технологий и особенностей функционирования ИСПДн.

С учётом перечисленных факторов, из базового набора мер, определённых для анализируемой ИСПДн, исключаем меры не соответствующие указанным характеристикам.

2.4.1 Анализ информационной системы персональных данных ФБУ «ЦСМ»

На рисунке 4 представлена ИСПДн «ЦСМ».

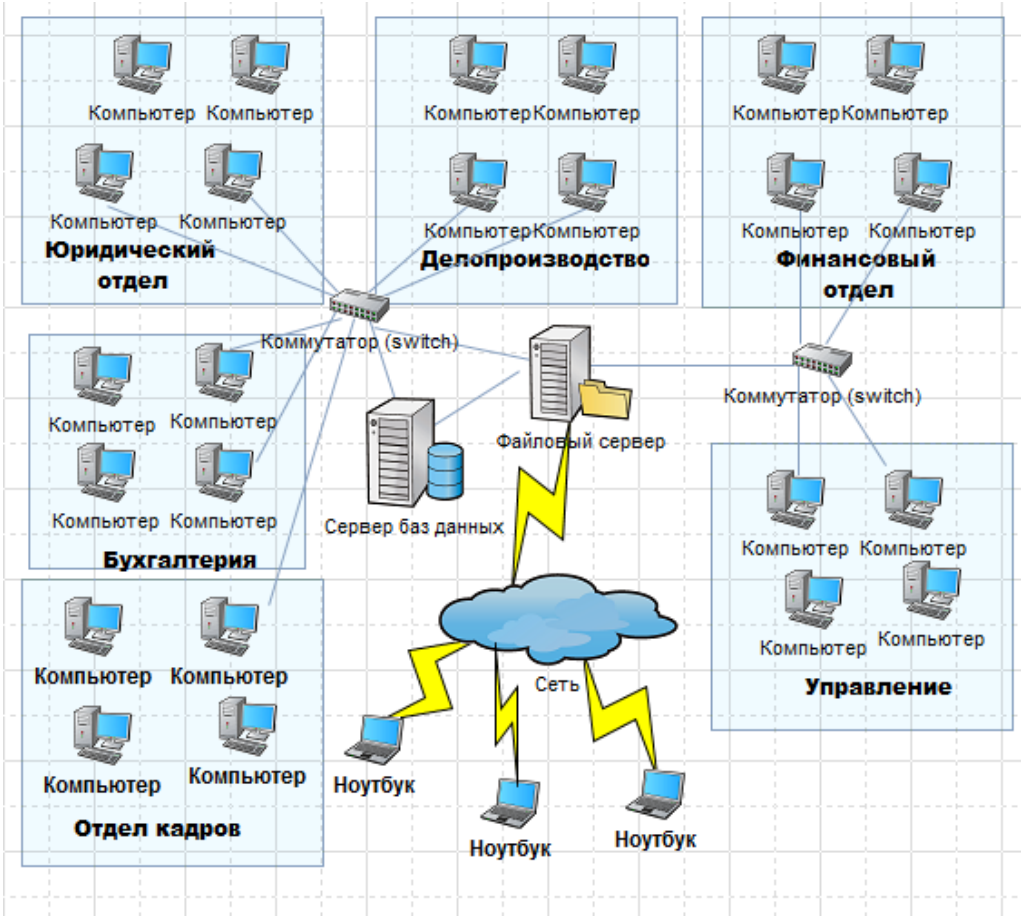

Рисунок 4 – Информационная система ПДн «ЦСМ»

Состав и назначение ИСПДн. «ЦСМ» представлены в таблице 18.

Таблица 18 – Состав и назначение ИСПДн «ЦСМ»

№ п/п	Название ИСПДН	Назначение ИСПДн
1	«1С»	Управление финансовой и хозяйственной деятельностью, ведение статистики.
2	«Кадры»	Управление персоналом, ведение статистики.
3	«Зарплата»	Расчет заработной платы, ведение статистики

ИСПДн предприятия расположена в отдельно стоящем здании с двумя выходами (основным и пожарным). На выходах установлены металлические двери, СКУД установлен. Охрана здания осуществляется ЧОП. Пост ЧОП расположен при входе в здание. В комплексе помещений развернута пожарная сигнализация и система оповещения.

Все сервера реализованы на серверах организации и установлены в серверном помещении, которое расположено в отдельном помещении. На серверах установлены ОС: Ubuntu 10.04, Windows Server 2003/2008.

Рабочие места расположены в общем свободном пространстве (Open Space) помещений, в который имеют доступ посетители и все сотрудники организации. На рабочих станциях используются ОС: Windows 7,10.

Техническое обслуживание ИТ–инфраструктуры осуществляет системный администратор.

Характеристики ИСПДн «ЦСМ» представлены в таблице 19.

Таблица 19 – Характеристики ИСПДн «ЦСМ»

№ п/п	Наименование ИСПДн	Разграничение прав доступа	Подключение к ССОП	Режим обработки ПДн	Структура ИСПДн
1.	«1С»	Имеет РПД	Да	МП	Локальная
2.	«Кадры»	Имеет РПД	Да	МП	Локальная
3.	«Зарплата»	Имеет РПД	Да	МП	Локальная

Таким образом, ИСПДн предприятия, это ЛВС, имеющая подключение к сетям связи общего пользования и сетям международного информационного

обмена, с разграничением прав доступа. Состав ПДн в ИСПДн «ЦСМ» представлен в таблице 20.

Таблица 20 – Состав ПДн, обрабатываемых в ИСПДн «ЦСМ»

№ п/п	ПДн	Наименование ИСПДн		
		«1С»	«Кадры»	«Зар-плата»
1.	Фамилия, имя, отчество (ФИО)	+	+	+
2.	Паспортные данные	+	+	–
3.	Дата и место регистрации	+	+	–
4.	Номер телефона адрес электронной почты	+	+	–
5.	Адрес фактического проживания	–	–	–
6.	Сведения об образовании	–	+	–
7.	Сведения о воинской службе	–	+	–
8.	Сведения о банковских счетах	+	–	+
9.	ИНН, СНИЛС, номер страхового полиса	+	–	+
10.	Сведения о родственниках	+	+	+
11.	Гражданство	–	+	–
12.	Дата и место рождения	+	+	–
13.	Записи трудовой книжки	–	+	–
14.	Пол	+	+	–
15.	Категория незанятости	–	–	–
16.	Стаж работы	+	+	+

Основой ИСПДн «ЦСМ» является компьютерная сеть организации. Внутренняя компьютерная сеть состоит из рабочих станций пользователей, которые через сетевое оборудование объединены в ЛВС и подключены к серверу. Сервер хранит всю информацию о деятельности предприятия и предоставляет ее при необходимости пользователям, посредством запросов. Вся сеть делится на три локальные сети, в зависимости от отдела, которые не

соединены между собой напрямую и взаимодействуют только через сервер организации [9].

Все объекты организации, на которых размещены компоненты ИСПДн, находятся на территории одного здания.

При входе в систему и выдаче запросов на доступ проводится аутентификация пользователей ИСПДн. Все пользователи разделены на группы по праву и уровню доступа: администратор ИСПДн, администратор безопасности, операторы АРМ с правом записи, операторы АРМ с правом чтения.

В таблице 21 – представлены СФХ ИСПДн предприятия.

Таблица 21 – Анализ структурно–функциональных характеристик ИСПДн организации

Анализируемые СФХ	СФХ реализованные в ИСПДн предприятия
Технологии, применяемые в составе системы	ЛВС
	мобильные устройства
свойства архитектуры	система на основе тонкого клиента
	система с удаленным доступом пользователей
	система с прикладными про–граммами, независимыми от ОС
взаимодействие с внешними системами	взаимодействует
подключение к сети	подключена
подключение к сети общего пользования	подключена через выделенную инфраструктуру
размещение компонентов системы по отношению к контролируемой зоне	в пределах одной контролируемой зоны
режим обработки информации в системе	многопользовательский
разграничение прав доступа к системе	разграничиваются
разделение функций по управлению информационной системой	рабочие места для администрирования выделены в отдельный домен
сегментирование ИС	сегментирована

Таблица 22– Названия и версии основного системного и прикладного ПО используемого в ИСПДн

Название и версия ПО	Назначение ПО	Места установки ПО	Тип ПО (системное или прикладное)
Microsoft Windows Server Standard 2008 R2 SP1	ОС сервера ИСПДн	Сервер s19–003	Системное
Microsoft Windows 7 Professional SP3	ОС АРМ ИСПДн	АРМ ИСПД	Системное
Microsoft SQL Server 2008 R2	СУБД ИСПДн	Сервер s19–003	Системное
«1С», «Кадры», «Зарплата»	Прикладное ПО ИСПДн (серверная часть)	Сервер s19–003	Прикладное
Microsoft Windows 7 Professional SP3	Прикладное ПО ИСПДн (клиентская часть ИСПДн)	АРМ ИСПДн	Прикладное

В результате адаптации базового набора мер, с учётом анализа ИСПДн и применяемых информационных технологий, сделан вывод, что из состава базового набора мер можно исключить меры, не соответствующие СФХ ИСПДн

Уточнение адаптированного базового набора мер

2.5.1 Модель вероятного нарушителя

С учетом всех исключений, в рамках настоящей Модели угроз предполагается, что к вероятным нарушителям ИСПДн будут относиться следующие лица (таблица 23).

Таблица 23 – Перечень вероятных нарушителей информационной безопасности ИСПДн организации

Вид нарушителя	Тип нарушителя	Функциональная характеристика нарушителя
Внешний	Тип 1	– отдельные лица, ведущие злоумышленную деятельность, не имеющие доступа в КЗ
Внутренний	Тип 2	- определенные категории обсуживающего персонала и представителей ремонтных организаций, не имеющих доступ к ИСПДн,
	Тип 3	представители технических и обслуживающих служб, консультационных и других вспомогательных служб, находящихся в пределах КЗ на постоянной основе или периодически (не имеют права доступа к техническим средствам и программному обеспечению ИСПДн)
	Тип 4	сотрудники организации, не являющиеся операторами или администраторами ИСПДн

Вид нарушителя	Тип нарушителя	Функциональная характеристика нарушителя
	Тип 5	сотрудник, являющийся оператором АРМ ИСПДн

Тип 6 не рассматривается в настоящей модели. Предполагается, что администраторы являются доверенными лицами и не относятся к категории нарушителей. Их доверенность должна обеспечиваться комплексом организационных мер по подбору персонала, закреплению ответственности и контролю лояльности.

Тип 7 сотрудники организаций, осуществляющих обслуживание узлов на постоянной основе в соответствии с заключенными договорами (не рассматривается в настоящей модели, предполагается, что защита от данного типа нарушителя обеспечивается комплексом организационно–технических мер).

Так же в рамках данной Модели угроз предполагается, что возможность сговора внутренних нарушителей, а также внутренних и внешних нарушителей, маловероятна, ввиду принятых организационных и контролирующих мер.

2.5.1.1 Предположения об имеющейся у нарушителя информации

Предположения об имеющейся у нарушителя информации приведены в таблице 24.

Таблица 24 – Предположения об имеющейся у нарушителя информации

Возможные виды потенциально опасной информации	Имеющаяся у нарушителя информация
Сведения о парольной и аутентифицирующей информации системы	Не обладает, но предполагается, что внутренний нарушитель обладает, сведениями о собственной аутентифицирующей информации
Планы зданий, мест размещения технических средств с привязкой к конкретным помещениям	Обладает частично
Данные о составе пользователей	Достоверной информацией не обладает
Сведения об информационных ресурсах узлов – порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков	Достоверной информацией не обладает
Данные об организации работы, структуре и используемых технических, программных и	Только имеющиеся в свободном доступе (например, сети Интернет)

Возможные виды потенциально опасной информации	Имеющаяся у нарушителя информация
программно–технических средствах узлов, в том числе тождественные проектной, конструкторской, программной и эксплуатационной документации на все компоненты узлов	
Все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно–техническими мерами	Достоверной информацией не обладает
Долговременные ключи криптосредств	Не обладает
Данные об уязвимостях СПО и ППО	Только описания, имеющиеся в свободном доступе (например, сети Интернет)
Сведения о возможных для данного узла каналах атак	Достоверной информацией не обладает
Информация о способах (методах) атак	Только описания, имеющиеся в свободном доступе (например, сети Интернет, печатных изданиях)
Данные об организациях осуществляющих поставку, ремонт, пуско-наладочные и монтажные работы, обслуживание технических и программных средств	Только сведения, имеющиеся в свободном доступе (например, сети Интернет)
Данные о местах ремонта и обслуживания технических средств узлов	Только сведения, имеющиеся в свободном доступе (например, сети Интернет)
Общая информированность нарушителя	Нарушитель 1 типа не обладает достоверной информацией об объекте и порядке обработки информации. Нарушители 2, 3, 4 типов обладают определенной информацией о структуре объектов Нарушитель 5 типа имеет представление об особенностях обработки информации на объектах, однако не имеет достоверной информации и не имеет сведений об используемых сетях связи.

2.5.1.2 Предположения об имеющихся у нарушителей средствах атак

Предположения об имеющихся у нарушителей средствах атак приведены в таблице 25.

Таблица 25 – Предположения об имеющихся у нарушителей средствах атак

№ п/п	Возможные средства атак	Имеющиеся у нарушителя средства атак
1.	Аппаратные компоненты криптографических средств	Отсутствует

№ п/п	Возможные средства атак	Имеющиеся у нарушителя средства атак
2.	Доступные в свободной продаже технические средства и программное обеспечение	Возможно применение подобных средств (включая общедоступные компьютерные вирусы)
3.	Специально разработанные технические средства и программное обеспечение	Отсутствует
4.	Штатные средства	Штатные средства размещены в пределах КЗ
5.	Распределенные ресурсы различных сетей, в том числе сети Интернет	Возможно организация распределенных атак

2.5.1.3 Предположения о каналах атак

Возможные каналы атак ограничены следующими предположениями:

– доступ в КЗ регламентирован и контролируется соответствующим режимом,

– в пределах КЗ серверное оборудование, каналы связи и коммуникационное оборудование доступно только для администраторов,

– обслуживающий персонал, при работе в помещениях где расположены компоненты системы, сотрудники, не являющиеся пользователями, находятся в помещениях с компонентами узлов только в присутствии сотрудников узлов,

– внутренний нарушитель (тип 5) самостоятельно осуществляет создание методов и средств реализации атак, а также самостоятельно реализует атаки. При этом внутренний нарушитель данного типа не имеет прямых возможностей доступа к средствам криптографической защиты информации других компонентов ИС, так как доступ ограничивается межсетевыми экранами, настройками СПО и ППО, вследствие чего его возможности по доступу к СКЗИ соответствуют возможностям нарушителя типа 4.

Основными каналами атак являются:

– внешние каналы связи, не защищенные от НСД к информации организационно–техническими мерами,

– штатные средства,

– каналы непосредственного доступа к объекту атаки (визуальный, физический),

– машинные носители информации,

– носители информации, выведенные из употребления.

Каналы атак, связанные с получением информации по ПЭМИН, через устройства негласного съема информации отсутствуют ввиду имеющихся у нарушителей средств атак и предположений об актуальности угроз.

Доступ к информационным и управляющим интерфейсам СВТ ограничен ввиду введенных предположений о возможностях нарушителя.

2.5.2 Определение актуальных угроз для ИСПДн предприятия

В таблице 26 представлены результаты оценки исходного уровня защищённости ИСПДн предприятия.

Таблица 26 – Характеристики уровня исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДН организации		Уровень защищенности		
Типы характеристик	Характеристики ИСПДн	Высокий	Средний	Низкий
По территориальному размещению	локальная ИСПДн, развернутая в пределах одного здания		–	–
По наличию соединения с сетями общего пользования	ИСПДн, имеющая одноточечный вход в сеть общего пользования	–	–	
По встроенным (легальным) операциям с записями баз ПДн	чтение, поиск, передача		–	–
По разграничению доступа к персональным данным	ИСПДн, к которой имеет доступ определенный перечень работников либо субъект ПДн	–	–	
По наличию соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая предприятию			
По уровню обобщения (обезличивания) ПДн	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	–		–
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн	–		–

ВЫВОД: ИСПДн имеет средний уровень исходной защищенности, так как более 70% характеристик соответствуют уровню не ниже «средний». Показатель исходной защищенности Y1= 5.

В таблице 27 представлены результаты работы по определению актуальных угроз с учётом исходного уровня защищённости ИСПДн.

Таблица 27 – Результаты работы по определению актуальных угроз для ИСПДн предприятия

№ п/п	Тип угроз безопасности ПДн	Коэффициент вероятности реализации	Вероятность возникновения угрозы	Коэффициент реализуемости угрозы	Возможность Реализации угрозы	Опасность угрозы	Актуальность угрозы
Угрозы утечки по техническим каналам							
Угрозы утечки видовой информации							
1.	Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке ПДн		средняя		средняя	высокая	актуальна
2.	Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн		низкая		средняя	низкая	неактуальна
3.	Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися за пределами помещения, в котором ведется обработка ПДн		маловероятно		низкая	низкая	неактуальна
Угрозы утечки акустической информации							
В ИСПДН функции голосового ввода ПДн в ИСПДн или функции воспроизведения ПДн акустическими средствами отсутствуют, поэтому детальное рассмотрение данной угрозы представляется нецелесообразным							
Угрозы утечки информации по каналам ПЭМИН.							
Угроз безопасности ПДн, связанных с перехватом ПЭМИН, избыточно, так как утечка ПДн по каналам ПЭМИН – маловероятна из–за несоответствия стоимости средств съема информации и полученной в результате регистрации ПЭМИН информации, а защита ПДн от данного вида угроз – экономически нецелесообразна.							
Угрозы НСД							

№ п/п	Тип угроз безопасности ПДн	Коэффициент вероятности реализации	Вероятность возникновения угрозы	Коэффициент реализуемости угрозы	Возможность Реализации угрозы	Опасность угрозы	Актуальность угрозы
Угрозы, реализуемые при физическом доступе							
4.	Кража ПЭВМ		маловероятна		низкая	средняя	неактуальна
5.	Вывод из строя узлов ПЭВМ, каналов связи		средняя		средняя	средняя	актуальна
6.	Кража элементов (жесткий диск) ПЭВМ		маловероятна		средняя	низкая	неактуальна
7.	Несанкционированный доступ к информации при техническом обслуживании (ремонте, модернизации) ПЭВМ		низкая		средняя	низкая	неактуальна
8.	Кража ключей от помещений, сейфов		низкая		средняя	низкая	неактуальна
9.	Кража носителей ключевой информации		низкая		низкая	средняя	неактуальна
10.	Кража индивидуальных устройств идентификации		низкая		средняя	низкая	неактуальна
Угрозы, возникающие при использовании съемных носителей ПДн							
11.	Кража съемных носителей ПДн		маловероятна		низкая	средняя	неактуальна
12.	Использование не учтенных носителей ПДн		средняя		средняя	средняя	актуальна
13.	Утрата съемных носителей ПДн		средняя		средняя	средняя	актуальна
Угрозы внедрения программных закладок							
14.	Компьютерные вирусы		высокая		средняя	высокая	актуальна

№ п/п	Тип угроз безопасности ПДн	Коэффициент вероятности реализации	Вероятность возникновения угрозы	Коэффициент реализуемости угрозы	Возможность Реализации угрозы	Опасность угрозы	Актуальность угрозы
15.	Несанкционированная модификация или уничтожение защищаемой информации		средняя		средняя	высокая	актуальна
16.	Несанкционированный перенос защищаемой информации на твердую копию		низкая		средняя	низкая	неактуальна
17.	Несанкционированный доступ внешних нарушителей к ресурсам ИСПДн		средняя		средняя	высокая	актуальна
18.	Загрузка ОС с внешних носителей (CD, DVD, USB Flash, внешний USB– винчестер и т. д.)		маловероятно		низкая	средняя	неактуальна
19.	Несанкционированное отключение средств защиты		маловероятно		низкая	средняя	неактуальна
Угрозы несанкционированного доступа по каналам связи							
20.	Перехват информации, передаваемой по локальной сети		средняя		средняя	средняя	актуальна
21.	Перехват информации, передаваемой по сетям международного обмена		средняя		средняя	средняя	актуальна
22.	Сканирование, направленное на выявление типа ОС, открытых портов и служб, открытых соединений и др.		низкая		низкая	средняя	неактуальна
23.	Подбор паролей через локальную вычислительную сеть организации или сети международного обмена		низкая		низкая	средняя	неактуальна
24.	Несанкционированный доступ через сети международного обмена		средняя		средняя	средняя	актуальна
25.	Несанкционированный доступ через локальную вычислительную сеть организации		средняя		средняя	средняя	актуальна

№ п/п	Тип угроз безопасности ПДн	Коэффициент вероятности реализации	Вероятность возникновения угрозы	Коэффициент реализуемости угрозы	Возможность Реализации угрозы	Опасность угрозы	Актуальность угрозы
26.	Несанкционированный удаленный запуск приложений		низкая		низкая	средняя	неактуальна
27.	Подмена доверенного объекта сети		низкая	2	низкая	средняя	неактуальна
28.	Внедрение ложного объекта		низкая	2	низкая	средняя	неактуальна
29.	Навязывание ложного маршрута		низкая		низкая	средняя	неактуальна
Угрозы непреднамеренных действий внутренних нарушителей							
30.	Непреднамеренная модификация или уничтожение информации сотрудниками, допущенными к ее обработке		средняя		средняя	средняя	актуальна
31.	Непреднамеренное отключение средств защиты		средняя		средняя	средняя	актуальна
32.	Утрата ключей от помещений, сейфов		низкая		низкая	средняя	неактуальна
33.	Утрата носителей ключевой информации		средняя		средняя	средняя	актуальна
34.	Утрата индивидуальных устройств идентификации		низкая		низкая	средняя	неактуальна
Угрозы не декларированных (недокументированных) возможностей							
35.	Угрозы, связанные с наличием не декларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн,		маловероятна		низкая	средняя	неактуальна
36.	Угрозы, связанные с наличием не декларированных возможностей в прикладном ПО, используемом в ИСПДн,		средняя		средняя	средняя	актуальна

№ п/п	Тип угроз безопасности ПДн	Коэффициент вероятности реализации	Вероятность возникновения угрозы	Коэффициент реализуемости угрозы	Возможность Реализации угрозы	Опасность угрозы	Актуальность угрозы
37.	Угрозы, не связанные с наличием не декларированных возможностей в программном обеспечении, используемом в ИСПДн		маловероятна		низкая	средняя	неактуальна
Угрозы неатропогенного характера							
38.	Сбой системы электроснабжения		высокая		средняя	средняя	актуальна
39.	Стихийное бедствие		средняя		низкая	средняя	неактуальна

Таблица 28 – Определение актуальности угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Перечень актуальных угроз, а также организационных и технических мер по их нейтрализации представлен в таблице 29.

Таблица 29 – Перечень актуальных угроз для ИСПДн «ЦСМ», а также организационных и технических мер по их нейтрализации

№ п/п	Наименование угрозы	Перечень организационных и технических
1.	Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке ПДн	ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее её несанкционированный просмотр ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
2.	Вывод из строя узлов ПЭВМ, каналов связи	ОДТ.3 Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению.
3.	Использование не учтенных носителей ПДн	ЗНИ.2 Управление доступом к машинным носителям ПДн .
4.	Утрата съемных носителей ПДн	ЗНИ.2 Управление доступом к машинным носителям ПДн. ОДТ.4 Периодическое резервное копирование ПДн на резервные машинные носители ПДн, ОДТ.5 Обеспечение возможности восстановления ПДн с резервных машинных носителей ПДн (резервных копий) в течение установленного временного периода,
5.	Компьютерные вирусы	АВЗ.1 Реализация антивирусной защиты, АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов), ЗСВ.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре,

№ п/п	Наименование угрозы	Перечень организационных и технических
		ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов. ОДТ.4 Периодическое резервное копирование ПДн на резервные машинные носители ПДн, ОДТ.5 Обеспечение возможности восстановления ПДн с резервных машинных носителей ПДн (резервных копий) в течение установленного временного периода,
6.	Несанкционированная модификация или уничтожение защищаемой информации	УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе и внешних пользователей, ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора.
7.	Несанкционированный доступ внешних нарушителей к ресурсам ИСПДн	ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены, ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора.
8.	Перехват информации, передаваемой по локальной сети	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами, УПД.14 Регламентация и контроль использования в информационной системе технологий беспроводного доступа, ЗИС.3 Обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе по беспроводным каналам, ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе.
9.	Перехват информации, передаваемой по сетям международного обмена	ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов. ЗИС.17 Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы

№ п/п	Наименование угрозы	Перечень организационных и технических
		управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
10.	Несанкционированный доступ через сети международного обмена	ЗИС.3 Обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе по беспроводным каналам, УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов. СОВ.1 Обнаружение вторжений, СОВ.2 Обновление базы решающих правил.
11.	Несанкционированный доступ через локальную вычислительную сеть организации	УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами, УПД.14 Регламентация и контроль использования в информационной системе технологий беспроводного доступа, ЗИС.3 Обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе по беспроводным каналам, ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе.
12.	Непреднамеренная модификация или уничтожение информации сотрудниками, допущенными к ее обработке	ОДТ.4 Периодическое резервное копирование ПДн на резервные машинные носители ПДн, ОДТ.5 Обеспечение возможности восстановления ПДн с резервных машинных носителей ПДн (резервных копий) в течение установленного временного периода,
13.	Непреднамеренное отключение средств защиты	УПД. 2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы,

№ п/п	Наименование угрозы	Перечень организационных и технических
		УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы, ЗИС.1 Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты ПДн , функции по обработке ПДн и иных функций информационной системы,
14.	Утрата носителей ключевой информации	ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов, АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователей в информационной системе
15.	Угрозы, связанные с наличием не декларированных возможностей в прикладном ПО, используемом в ИСПДН,	АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей, АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения и средств защиты информации, ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.
16.	Сбой системы электроснабжения	ОДТ.3 Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению.

2.6 Выбор средств реализации технических мер защиты в информационной системе персональных данных предприятия

Для построения СЗИ в ИС необходимо выбрать перечень средств защиты информации. С учётом перечня выбранных мер и определённого УЗ для ПДн АО к реализации предлагаются следующие средства защиты (таблица 30).

Таблица 30 – Перечень СЗИ для реализации технических мер защиты в ИСПДн организации

Группа мер	Средства защиты информации
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	АПКШ «Континент» 3,9
Управление доступом субъектов доступа к объектам доступа (УПД)	АПКШ «Континент» 3,9

Группа мер	Средства защиты информации
Ограничение программной среды (ОПС)	vGate - S SecretNet Studio
Защита машинных носителей информации (ЗНИ)	СЗИ от НСД SecretNet LSP
Регистрация событий безопасности (РСБ)	АПКШ «Континент» 3.9
Антивирусная защита (АВЗ)	SecretNet Studio
Обнаружение (предотвращение) вторжений (СОВ)	СОВ Континент (детектор атак)
Контроль (анализ) защищенности информации (АНЗ)	СЗИ от НСД SecretNet LSP
Целостность информационной системы и информации (ОЦЛ)	Соболь
Доступность технических средств и информации (ОДТ)	АПКШ «Континент» 3.9
Защита среды виртуализации (ЗСВ)	Не реализована
Защита технических средств и оборудования (ЗТС)	Применяемые на объекте системы физической охраны (видеонаблюдение, СКУД и пр).
Защиту автоматизированной системы и ее компонентов (ЗИС)	АПКШ «Континент» 3.9
Выявление инцидентов и реагирование на них (ИНЦ)	АПКШ «Континент» 3.9
Управление конфигурацией информационной системы и системы защиты ПДн(УКФ)	Периодический анализ уровня защищённости ИСПДн и управление конфигурацией по ситуации

Требования к техническим средствам и системам защиты представлены в таблице 31[5].

Таблица 31– Соответствие класса защиты средства ЗИ в ИСПДн для 3УЗ

Уровень защищённости ПДн	Класс защиты СЗИ						Уровень контроля на отсутствие не декларированных возможностей
	СВТ	САВЗ	СОВ	МЭ	СДЗ	СЗИ	
УЗ 3	Не ниже 5 класса	Не ниже 4 класса	Не ниже 4 класса	Не ниже 3 класса	Не ниже 4 класса	Не ниже 6 класса	4 уровень контроля
Требования к сертификации	Использовать сертифицированные по требованиям безопасности информации СВТ и СЗИ						

Для обеспечения защиты ПДн, содержащейся в ИСПДн, применяются СВТ, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184–ФЗ «О техническом регулировании» [18].

2.7 Выводы по второму разделу

Во втором разделе проведена апробация предложенных рекомендаций по построению СЗПДн для конкретной организации «ЦСМ». По результатам работы можно сделать вывод, что использование предложенных рекомендаций позволило:

– оптимизировать последовательность работ по построению СЗПДн в ИСПДн,

– учесть требования нормативных документов, при проведении различных этапов данной работы,

– определить перечень организационных и технических мер защиты ПДн в ИСПДн, а также выбрать средства реализации технических мер защиты.

3 Оценка эффективности предложенных рекомендаций и технико - экономическое обоснование возможности их реализации в системе защиты персональных данных

3.1 Сравнительная оценка эффективности системы защиты персональных данных в информационной системе персональных данных

Результаты представлены в таблицах 32…38.

Таблица 32 – Оценка наличия и содержания ОРД по защите ПДн разработанных в организации

Нормативные документы по ИБ ПДн организации	Соответствие	
	до	после
Федеральный закон от 27.07.2006 N 149–ФЗ «Об информации, информационных технологиях и о ЗИ»	0,5	0,5
Федеральный закон от 27 июля 2006 г. N 152–ФЗ «О ПДн »	0,5	1
Приказ ФСТЭК России от 18 февраля 2013 г. N 21 Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн	0	1
Базовая модель угроз безопасности ПДн при их обработке в информационных системах ПДн (выписка). ФСТЭК России, 2008 год	0	1
Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах ПДн . ФСТЭК РФ, 2008 год	0	1
перечень сведений конфиденциального характера	1	1
перечень ПДн , подлежащих защите	0	1
инструкция администратора информационной безопасности	1	1
приказ о назначении лиц, ответственных за организацию обработки ПДн и перечне мер по защите ПДн	0	1
приказ о введении режима обработки ПДн	0	1
приказ об утверждении мест хранения ПДн	0	1
приказ о назначении комиссии по уничтожению ПДн	0	1
порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации	0	0
план внутренних проверок режима защиты ПДн	0	0
приказ о вводе в эксплуатацию информационной системы ПДн	0	0

Нормативные документы по ИБ ПДн организации	Соответствие	
	до	после
журнал учета носителей информации информационной системы ПДн	1	1
журнал учета мероприятий по контролю обеспечения защиты ПДн	0	1
журнал учета обращений граждан–субъектов ПДн о выполнении их законных прав	1	1
положение о разграничении прав доступа к обрабатываемым персональным данным	0	1
инструкция по проведения антивирусного контроля в информационной системе ПДн	0	1
инструкция пользователя ИСПДН	1	1
инструкция администратора ИСПДн	1	1
инструкция по организации парольной защиты	1	1
журнал периодического тестирования средств защиты информации	0	0
акты уничтожения документов, содержащих персональные данные	0	0
соглашение о неразглашении ПДн	1	1
журнал учета средств защиты информации	1	1
журнал проведения инструктажа по информационной безопасности	0	1
инструкция пользователю по обеспечению безопасности при возникновении внештатных ситуаций	0	0
приказ о перечне лиц, допущенных к обработке ПДн	1	1
положение об обработке и защите ПДн	1	1
план мероприятий по обеспечению безопасности ПДн	0	1
модель угроз безопасности в информационной системе ПДн	0	1
ИТОГО	12	26

Результат оценки определяется по соответствующему значению таблицы 33.

Таблица 33– Определение коэффициента R_n.

% выполнения требований нормативных документов	Риск несоответствия требованиям законодательства (Rn)
91–100	0,01
61–90	0,25
21–60	0,5

≤ 20	0,9

Таким образом, значение $Rn_1 = 0,25$, $Rn_2 = 0,01$.

Этап 2 Определение вероятности реализации хотя бы одной из актуальных угроз для ИСПДн.

На основании частной модели угроз для ИСПДН организации определён перечень актуальных угроз и вероятности их реализации (таблица 34).

Таблица 34 – Перечень актуальных угроз для ИСПДн и вероятностей их реализации

Тип угроз безопасности ПДн	Вероятность реализации угрозы до внедрения СЗПДн (Y до внедрения СЗПДн)	Вероятность реализации угрозы после внедрения СЗПДн (Y после)
Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке ПДн	0,5	0,25
Вывод из строя узлов ПЭВМ, каналов связи	0,5	0,25
Использование не учтенных носителей ПДн	0,35	0,25
Утрата съемных носителей ПДн	0,35	0,25
Компьютерные вирусы	0,35	0,25
Несанкционированная модификация или уничтожение защищаемой информации	0,35	0,25
Несанкционированный доступ внешних нарушителей к ресурсам ИСПДН	0,35	0,25
Перехват информации, передаваемой по локальной сети	0,35	0,25
Перехват информации, передаваемой по сетям международного обмена	0,25	0,25
Несанкционированный доступ через сети международного обмена	0,35	0,25
Несанкционированный доступ через локальную вычислительную сеть организации	0,35	0,25
Непреднамеренная модификация или уничтожение информации сотрудниками, допущенными к ее обработке	0,35	0,25
Непреднамеренное отключение средств защиты	0,35	0,25

Тип угроз безопасности ПДн	Вероятность реализации угрозы до внедрения С 3	Вероятность реализации угрозы после внедрения СЗПДн Y после)
Утрата носителей ключевой информации	0,35	0,25
Угрозы, связанные с наличием не декларированных возможностей в прикладном ПО, используемом в ИСПДН,	0,35	0,25
Сбой системы электроснабжения международного обмена	0,35	0,25

Вероятность реализации хотя бы одной угрозы из совокупности вероятностей угроз Р*у*1, Р*у*2, ..., Р*уn*, равна разности между единицей и произведением вероятностей противоположных событий. Вероятность противоположных событий определяется как разность между единицей и вероятностью угроз.

$$P_{угр} = 1 - П(1 - P_{у1})(1 - P_{у2})(1 - P_{у3})...(1 - P_{уn}) \quad (1)$$

где n–количество угроз.

$$Ругр = 1 - П(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}25)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}25)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}35)(1 - 0{,}25)(1 - 0{,}35) = 0{,}696.$$

В результате проведённых расчётов вероятность реализации угроз по основным типам объектов среды:

$$Р_{угр\ 1} = 0{,}696,\ Р_{угр\ 2} = 0{,}52.$$

Этап 3. Определение ценности ПДн обрабатываемых в ИСПДн

Ценность ПДн С, определяется отношением стоимости ПДн обрабатываемых в ИСПДн к стоимости всей организации. В общем случае., можно принять С = 0,5.

Этап 3. Определение степени использования организационных и технических средств защиты ПДн В ИСПДн

В ходе проведения анализа, всем организационным мерам, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются (таблица 35).

Таблица 35 – Анализ степени выполнения организационных мер защиты ПДн в ИСПДн «ЦСМ»

Организационные меры защиты информации	Соответствия	
	до	после
Назначение ответственного за организацию обработки ПДн	0	1
Назначение администратора безопасности ПДн	1	1
Организация контролируемой зоны	0	1
Контроль перемещения машинных носителей ПДн за пределы КЗ	0	1
Контроль и управление физическим доступом к техническим средствам, средствам защиты ПДн	0	1
Определение лиц, допущенных к обработке ПДн	1	1
Определение категории ПДн, которые подлежат защите	1	1
Положение по обработке и защите ПДн.	0	1
Реализация механизмов регистрации событий, связанных с действиями пользователя	0	0
Управление доступом к машинным носителям ПДн	1	1
Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн	1	1
Учет машинных носителей ПДн	1	1
Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИСПДн	1	1
Определение лиц, которым разрешены действия по внесению изменений в конфигурацию ИСПДн и системы защиты ПДн	0	1
Ограничение прав пользователей по вводу информации в ИСПДн	1	1
Инструкция по организации антивирусной защиты в ИСПДН	1	1

Правила рассмотрения запросов ПДн или их представителей	0	0
Проверка системного и (или) прикладного ПО на отсутствие не декларированных возможностей	0	1
Контроль доступа к внешним устройствам	1	1
Положение о разграничении прав доступа к обрабатываемым ПДн	1	1
Модели угроз безопасности ПДн	0	1
План мероприятий по обеспечению защиты ПДн	1	1
План внутренних проверок состояния защиты ПДн	0	1
Обнаружение вторжений	0	0
Проект договора о поручении обработки ПДн третьим лицам	0	0
Согласие субъекта на обработку ПДн	1	1
Итого	13	21

Результат оценки определяется по соответствующему значению таблицы 36.

Таблица 36 – Определение коэффициента использования организационных мер защиты k_o

% выполнения организационных мер защиты	Значение коэффициента (Rn)
91–100	0,01
61–90	0,25
21–60	0,5
≤ 20	0,9

Таким образом, коэффициент уязвимости организационных мер защиты информации Ко1 = 0,5, Ко2 = 0,25.

Возможность использования технических уязвимостей проводилась экспертным методом, анализируя применяемые технические меры защиты информации. В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», частично выполняются – «0,5» не выполняются – «0». Все значения, которым присвоено значение 0,5 и 1, суммируются, остальные значения не учитываются. В таблицах 37, 38

представлены коэффициент уязвимости технических мер защиты информации и соответствие выполняемых технических мер защиты информации требуемым соответственно.

Таблица 37 – Анализ степени выполнения технических мер защиты ПДн в ИС-ПДн «ЦСМ»

Перечень технических мер защиты	до	после
ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее её несанкционированный просмотр	1	1
ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации	0	1
ЗТС.3 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены	1	1
ОДТ.3 Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению.	0	1
ОДТ.4 Периодическое резервное копирование ПДн на резервные машинные носители ПДн ,	1	1
ОДТ.5 Обеспечение возможности восстановления ПДн с резервных машинных носителей ПДн (резервных копий) в течение установленного временного периода,	0	1
ЗНИ.2 Управление доступом к машинным носителям ПДн .	0	1
АВЗ.1 Реализация антивирусной защиты,	0	1
АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов),	1	1
ЗСВ.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре	1	1
ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	0	1
УПД.3 Управление информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами,	1	1
УПД.14 Регламентация и контроль использования в информационной системе технологий беспроводного доступа,	0	1
УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы,	1	1
УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	1	1

Перечень технических мер защиты	до	после
УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе и внешних пользователей,	1	1
УПД. 2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	0	1
ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора.	0	1
ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	1	1
ЗИС.1 Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты ПДн , функции по обработке ПДн и иных функций информационной системы	0	1
ЗИС.3 Обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе по беспроводным каналам,	0	1
ЗИС.17 Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	1	1
ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов.	1	1
ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе.	0	1
СОВ.1 Обнаружение вторжений	1	1
СОВ.2 Обновление базы решающих правил.		1
АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей,	1	1
АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа	0	1
АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения и средств защиты информации	0	1
ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.	0	1
Итого	15	28

Результат оценки определяется по соответствующему значению таблицы 38.

Таблица 38 – Определение коэффициента использования технических мер защиты ПДн ($k_{t)}$

% выполнения технических мер защиты	Значение коэффициента (K_t)
91–100	0,01
61–90	0,25
21–60	0,5
≤ 20	0,9

Расчёты показали, что $K_t1 = 0,5$, $K_t2 = 0,01$.

Этап 4. Количественное определение риска.

Итоговая формула определения риска ИБ для ИСПДн имеет вид [8]:

$$R = P_{\text{угр}} \cdot R_n \cdot C \cdot \frac{K_o + K_t}{2} \cdot 100\%, \quad (2)$$

где *R* – численная величина риска реализации угроз ИБ,

*P*угр – вероятность реализации хотя бы одной угрозы из всего перечня угроз,

Rn – риск несоответствия требованиям законодательства в области информационной безопасности,

C – ценность актива (0…1),

Ko – вероятность использования организационных уязвимостей,

Kt – вероятность использования технических уязвимостей.

$$R_1 = 0.996 \cdot 0.5 \cdot 0.5 \cdot (0.5 + 0.5)/2 \cdot 100\% = 8.4\%$$

$$R_2 = 0,95 \cdot 0,01 \cdot 0,5 \cdot (0.25 + 0.01)/2 \cdot 100\% = 3,27\%.$$

Сравнительный анализ риска ИБ представлен на рисунке 5.

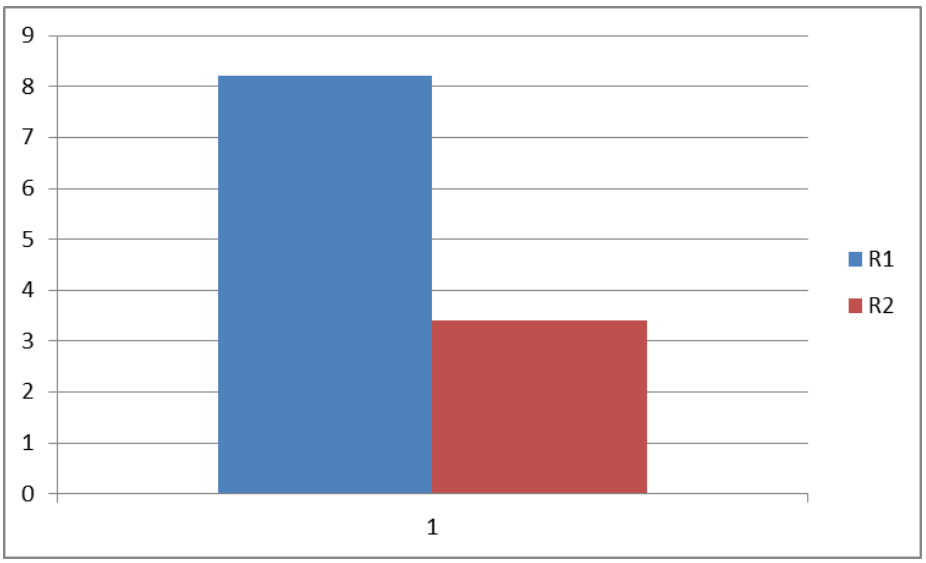

Рисунок 5 – Значение риска ИБ по основным каналам утечки информации

Как видно из анализа результатов риск ИБ для ИСПДн центра снизился приблизительно на 5 %.

3.2 Технико - экономическое обоснование возможности реализации предложенных рекомендаций

Технико - экономическое обоснование проводилось по критерию определения суммы материальных затрат на реализацию предложенных мероприятий по построению СЗПДн организации.

Спецификация оборудования и работ по созданию СЗПДн организации представлена в таблице 39.

Таблица 39 – Спецификация затрат на реализацию предложенных рекомендаций для СЗПДн предприятия

№ п/п	Наименование средства/меры	Цена одного комплекта	Количество потребителей	Стоимость
1.	АПКШ «Континент» 3.9 IPC-100	320230	500	320230
2.	СЗИ от НСД SecretNet	8230	1	8230
3.	SecretNet Studio	15000	1	15000
4.	СОВ Континент IPC-100ND	391170	1	391170
5.	ПАК Соболь М.2	12128	1	12128
Итого				746758

Таким образом, можно сделать вывод, что общая сумма затрат на модернизацию СЗИ для ИСПДн составит 746758 рублей.

3.3 Вывода по разделу

В третьем разделе:

– по критерию сравнительного анализа величины риска ИБ для ИСПДн предприятия, до и после реализации СЗПДн в ИСПДн проведена оценка эффективности СЗПДн в ИСПДн. Как видно из анализа результатов, риск ИБ для ИСПДн «ЦСМ» снизился на 5%,

– проведено технико - экономическое обоснование результатов работы.

Расчёты показали, что затраты на реализацию предложенных средств технической защиты составят около 746758 рублей.

ЗАКЛЮЧЕНИЕ

В результате проведённых исследований:

– проведён анализ требований нормативно–методических документов, регламентирующих порядок построения СЗПДн в ИСПДн,

– разработаны рекомендации оператору ПДн по построению СЗПДн в ИСПДн с учётом требований НМД,

– проведена апробация предложенных рекомендаций по построению СЗПДн в ИСПДн реальной организации «ЦСМ»,

– проедена сравнительная оценка эффективности СЗПДн, построенной с учётом разработанных рекомендаций, по выбранному критерию (величина риска ИБ для ИСПДн),

– проведено технико - экономическое обоснование возможности реализации предложенных рекомендаций по построению СЗПДн в ИСПДн организации.

Таким образом, можно сделать вывод, что значение риска ИБ для ИСПДн снизилось на 5 %, а затраты на создание СЗИ в ИСПДн организации составят около 746758 рублей.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Закон РФ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 № 149 – ФЗ. Российская газета. – 29.07. 2006. – С.22–34.

2 Закон РФ "О ПДн " от 27.07.2006 № 152 – ФЗ Бюллетень нормативных актов министерств и ведомств. – № 7. – 2006. – С.15–32.

3 Приказ ФСТЭК от 18.02.2013. № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн, при их обработке в информационных системах ПДн "

4 Постановление правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн ".

5 Базовая модель угроз безопасности ПДн при их обработке в информационных системах ПДн, утвержденная приказом ФСТЭК РФ 15.02.2008 г.

6 Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах ПДн, утверждена приказом ФСТЭК РФ 14.02.2008 г.

7 Постановление Правительства РФ от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О ПДн ".

8 ГОСТ 34.601–90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

9 ГОСТ 34.602–89 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

10 ГОСТ Р 51583–2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

11 ГОСТ Р 51275–2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

12 ГОСТ Р 50739–95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации».

13 ГОСТ 34.003–90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».

14 ГОСТ 34.201–89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

15 ГОСТ ИСО 15288. Проектирование систем — Процессы жизненного цикла системы.

16 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР–К), утвержденные Приказом Гостехкомиссии России от 30.08.2002 № 282.

17 Постановление Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации".

18 Информационное сообщение ФСТЭК «О банке данных угроз безопасности информации» от 6 марта 2015 г. N 40/22/879.

19 Коробейников Д.А., Османов А.А. К вопросу о процедуре выбора оператором ПДн перечня организационных и технических мер защиты ПДн в информационных системах ПДн: Сборник материалов Всероссийской научно–практической конференции / СКФУ. – Ставрополь: СКФУ, 2018. – С. 46–49.

ПРИЛОЖЕНИЕ А
(обязательное)

Перечень основных нормативно - методических документов, регламентирующих порядок разработки системы защиты в информационных системах персональных данных

Основные федеральные документы:

1. «Конституция РФ», принята всенародным голосованием 12 декабря 1993г.
2. «О Декларации прав и свобод человека и гражданина», Постановление Верховного Совета РСФСР от 22.11.1991 № 1920–1.
3. «Доктрина информационной безопасности РФ», утверждена Президентом РФ 9 сентября 2000г. №Пр–1895.

Кодексы:

4. «Уголовный кодекс РФ», принят Федеральным законом от 13 июня 1996г. № 63–ФЗ.
5. «Кодекс РФ об административных правонарушениях», принят Федеральным законом от 30 декабря 2001г. №195–ФЗ.
6. «Гражданский кодекс РФ (часть первая)», принят Федеральным законом от 30 ноября 1994г. №51–ФЗ.
7. «Гражданский кодекс РФ (часть вторая)», принят Федеральным законом от 26 января 1996г. №14–ФЗ.
8. «Гражданский кодекс РФ (часть третья)», принят Федеральным законом от 26 ноября 2001г. №146–ФЗ.
9. «Гражданский кодекс РФ (часть четвертая)», принят Федеральным законом от 18 декабря 2006г. №230–ФЗ.
10. «Трудовой кодекс РФ», принят Федеральным законом от 30 декабря 2001 г. № 197–ФЗ.
11. «Воздушный кодекс РФ» принят Федеральным законом от 19 марта 1997г. № 60–ФЗ. Статья 85.1. Персональные данные пассажиров воздушных судов.

Федеральные законы:

12. Федеральный Закон от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации».
13. Федеральный Закон от 11 июля 2011г. № 200–ФЗ «О внесении изменений в отдельные законодательные акты РФ в связи с принятием Федерального Закона «Об информации, информационных технологиях и о защите информации».
14. Федеральный Закон от 19 декабря 2005г. № 160–ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн».
15. Федеральный Закон от 27 июля 2006г. № 152–ФЗ «О ПДн».
16. Федеральный Закон от 29 июля 2004г. № 98–ФЗ «О коммерческой тайне».
17. Федеральный закон от 2 декабря 1990г. № 395–1 «О банках и банковской деятельности».
18. Федеральный закон от 4 мая 2011г. № 99–ФЗ «О лицензировании отдельных видов деятельности».

19. Федеральный закон от 6 апреля 2011г. № 63–ФЗ «Об электронной подписи».

20. Федеральный закон от 27 декабря 2002г. № 184–ФЗ «О техническом регулировании».

21. Закон РФ от 21 июля 1993г. № 5485–1 «О государственной тайне».

22. Федеральный закон от 7 июля 2003г. № 126–ФЗ «О связи».

Указы Президента РФ:

23. Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности РФ до 2020 года».

24. Указ Президента РФ от 6 марта 1997г. № 188 «Об утверждении перечня сведений конфиденциального характера» (в ред. Указа Президента РФ от 23 сентября 2005г. № 1111).

25. Указ Президента РФ от 30 мая 2005г. № 609 «Об утверждении Положения о ПДн государственного гражданского служащего РФ и ведении его личного дела».

26. Указ Президента РФ от 17 марта 2008г. № 351 «О мерах по обеспечению информационной безопасности РФ при использовании информационно–телекоммуникационных сетей международного информационного обмена».

27. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации.

Постановления Правительства РФ:

28. Постановление Правительства РСФСР от 5 декабря 1991г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

29. Постановление Правительства РФ от 16 марта 2009г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

30. Постановление Правительства РФ от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации».

31. Постановление Правительства РФ от 1 ноября 2012г. № 1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн».

32. Постановление Правительства РФ от 6 июля 2008г. № 512 «Об утверждении требований к материальным носителям биометрических ПДн и технологиям хранения таких данных вне информационных систем ПДн».

33. Постановление Правительства РФ от 4 марта 2010г. № 125 «О перечне ПДн, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина РФ, по которым граждане РФ осуществляют выезд из РФ и въезд в Российскую Федерацию».

34. Постановление Правительства РФ от 3 марта 2012г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».

35. Постановление Правительства РФ от 3 февраля 2012г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

36. Постановление Совета Министров – Правительства РФ от 15 сентября 1993г. № 912–51 «Об утверждении Положения о государственной системе защиты информации в РФ от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения).

37. Постановление Правительства РФ от 18 мая 2009г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно–телекоммуникационным сетям».

38. Постановление Правительства РФ от 26 июня 1995г. № 608 «О сертификации средств защиты информации».

39. Постановление Правительства РФ от 3 ноября 1994г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

40. Постановление Правительства РФ от 21 марта 2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О ПДн» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Нормативные документы ФСТЭК России:

41. «Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах ПДн», утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.

42. «Базовая модель угроз безопасности ПДн при их обработке в информационных системах ПДн (выписка)», утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.

43. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн», Приказ ФСТЭК России от 18 февраля 2013г. № 21.

44. «Методические рекомендации по технической защите информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.

45. «Пособие по организации технической защиты информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.

46. «Положение о сертификации средств защиты информации по требованиям безопасности информации», утверждено приказом председателя Государственной технической комиссии при Президенте РФ от 27 октября 1995г. № 199.

47. «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР–К)», утверждены приказом председателя Государственной технической комиссии при Президенте РФ от 30 августа 2002г. № 282.

48. «Методические документы по технической защите информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.

49. «Методические документы по обеспечению ПДн при их обработке в ИСПДн», утверждены Заместителем директора ФСТЭК России 14 февраля 2008г. и 15 февраля 2008г. и Приказом ФСТЭК России от 05 февраля 2010г. № 58.

50. «Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах ПДн», ФСТЭК России, 2008г., пометка «для служебного пользования» снята Решением ФСТЭК России от 16 ноября 2009г.

51. «Базовая модель угроз безопасности ПДн при их обработке в информационных системах ПДн (выписка)», (при рассмотрении угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) необходимо применять полную версию данного документа), ФСТЭК России, 2008г.

52. «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 18 мая 2007г.

53. «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 19 ноября 2007г.

Нормативные документы ФСБ России:

54. «Об утверждении Методических рекомендаций по обеспечению с помощью криптосредств безопасности ПДн при их обработке в информационных системах ПДн с использованием средств автоматизации», утверждены Приказом ФСБ РФ 21 февраля 2008г. № 149/54–144.

55. Приказ ФСБ РФ от 9 февраля 2005г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005)».

Стандарты:

56. ГОСТ Р 51275–99. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», принят и введен в действие Постановлением Госстандарта РФ от 12 мая 1999г. №160.

57. ГОСТ Р 50739–95. «Средства вычислительной техники. Защита от НСД к информации. Общие технические требования»

58. ГОСТ Р ИСО/МЭК 15408–1–2002. «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель». Госстандарт России.

59. ГОСТ Р ИСО/МЭК 15408–2–2002. «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности». Госстандарт России.

60. ГОСТ Р ИСО/МЭК 15408–3–2002. «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности». Госстандарт России.

61. ГОСТ Р 50922–96. «Защита информации. Основные термины и определения».

62. ГОСТ 28147–89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

63. ГОСТ Р 34.10–2001. «Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

64. ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утвержден и введён в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 года №375–ст). Дата введения: 01.02.2008.

65. ГОСТ Р ИСО/МЭК 27003 2012 «Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности» (утвержден и введён в действие приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 года №812–ст). Дата введения: 01.12.2013.

66. ГОСТ Р ИСО/МЭК 27004 2011 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения» (утвержден и введён в действие приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 года №681–ст). Дата введения: 01.01.2012.

67. ГОСТ Р ИСО/МЭК 27005 2010 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (утвержден и введён в действие приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 года №632–ст). Дата введения: 01.12.2011.

68. ГОСТ Р ИСО/МЭК 27006 2008 «Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности» (утвержден и введён в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 года №524–ст). Дата введения: 01.10.2009.

69. BS 7799 1. «Управление информационной безопасностью. Общие требования к управлению информационной безопасностью».

70. BS 7799 2. «Управление информационной безопасности. Требования и руководство по применению».

71. BS 7799 3. «Управление информационной безопасности. Руководство по управлению рисками информационной безопасности».

72. ISO/IEC 27001:2005. «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования».

73. ISO/IEC 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению информационной безопасностью».

74. ISO/IEC 27006:2007 «Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью».

ПРИЛОЖЕНИЕ Б

(обязательное)

ПЕРЕЧЕНЬ

персональных данных, являющихся объектом защиты ФБУ «ЦСМ»

УТВЕРЖДАЮ
Ген. директор ФБУ «ЦСМ»
В.А. Коршак
24.05.2020

№ п/п	Наименование сведений	Категория ПДн	Срок конфиденциальности	Перечень сотрудников допущенных к ПДн
1.	Фамилия, имя, отчество, день, месяц, год и место рождения	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
2.	Паспортные данные или данные иного документа, удостоверяющего личность	иные	постоянно	Сотрудник ОК и бухгалтерии
3.	Гражданство	иные	постоянно	Сотрудник ОК и бухгалтерии,
4.	Адрес места жительства и дата регистрации по месту жительства или по месту пребывания	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
5.	Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
6.	Сведения о повышении квалификации и переподготовке	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
7.	Сведения о трудовой деятельности	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
8.	Данные о трудовом договоре	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
9.	Сведения о номере, серии и дате выдачи трудовой книжкии записях в ней.	иные	постоянно	Сотрудник ОК и бухгалтерии,
10.	Сведения о заработной плате (номера счетов для расчета с Работниками, в том числе номера их банковских карточек)	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
11.	Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу	иные	постоянно	Сотрудник ОК и бухгалтерии

№ п/п	Наименование сведений	Категория ПДн	Срок конфиденциальности	Перечень сотрудников допущенных к ПДн
12.	Сведения о семейном положении	иные	постоянно	Руководители структурных подразделений, сотрудник ОК и бухгалтерии,
13.	Сведения о номере и серии страхового свидетельства государственного пенсионного страхования и ИНН	иные	постоянно	Сотрудник ОК и бухгалтерии
14.	Сведения из страховых полисов обязательного медицинского страхования	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
15.	Сведения, указанные в оригиналах и копиях приказов по персоналу	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
16.	Копии приказов, изданных в ЗАО, и относящиеся к субъекту персональных данных;	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
17.	Сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
18.	Материалы по аттестации и оценке Работников	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
19.	Материалы по внутренним служебным расследованиям в отношении работников	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
20.	Табельный номер работника	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
21.	Сведения о социальных льготах и о социальном статусе	иные	постоянно	Руководители СП, сотрудник ОК и бухгалтерии
22.	Персональные данные отнесённые к категории биометрических или специальных в ИСПДн не обрабатываются.			

Председатель ПДЭК А.В. Сухарев
Члены ПДЭК И.К. Тимофеева
М.П. Порсак

ПРИЛОЖЕНИЕ В
(обязательное)

Базовый набор мер для УЗ 3

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	ФБУ «ЦСМ» идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	ФБУ «ЦСМ» средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	ФБУ «ЦСМ» (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	ФБУ «ЦСМ» (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы ФБУ «ЦСМ») информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в ИС (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно–информационные сети

УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	ФБУ «ЦСМ» взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
III. Ограничение программной среды (ОПС) (нет для 3 уровня защищённости)	
IV. Защита машинных носителей ПДн(ЗНИ)	
ЗНИ.8	Уничтожение (стирание) или обезличивание ПДнна машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.З	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ. 7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VII. Обнаружение вторжений (СОВ) (нет для 3 уровня защищённости)	
VIII. Контроль (анализ) защищенности ПДн(АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
IX. Обеспечение целостности информационной системы и ПДн(ОЦЛ) (нет для 3 уровня) **X. Обеспечение доступности ПДн(ОДТ) (нет для 3 уровня)**	
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов ФБУ «ЦСМ» средствами виртуализации

ЗСВ.2	ФБУ «ЦСМ» доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.9	Реализация и ФБУ «ЦСМ» антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки ПДнотдельным пользователем и (или) группой пользователей
XII. Защита технических средств (ЗТС)	
ЗТС.3	Контроль и ФБУ «ЦСМ» физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты ПДнот раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
XIV. Выявление инцидентов и реагирование на них (ИНЦ) (нет для 3 уровня защищённости)	
XV. ФБУ «ЦСМ» конфигурацией информационной системы и системы защиты ПДн(УКФ)	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
УКФ.2	ФБУ «ЦСМ» изменениями конфигурации информационной системы и системы защиты персональных данных
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации ИС и СЗПд на обеспечение защиты ПДни согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных