

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03 –

Информационная безопасность
автоматизированных систем

Специализация -

Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ПРОЕКТ СИСТЕМЫ ЗАЩИТЫ СИСТЕМЫ ЭЛЕКТРОННОГО
ДОКУМЕНТООБОРОТА И ДЕЛОПРОИЗВОДСТВА ПЕНЗЕНСКОЙ ОБЛАСТИ

Студент

Авдониин Игорь Алексеевич

Руководитель



Комиссарова Н.А.

Нормоконтролёр

Фатеев А.Г.

Рецензент Начальник отдела

администрирования и отчетности

Управления цифрового развития,

информационных технологий и связи

Пензенской области

Тюрин Е.А.

Работа допущена к защите (протокол заседания кафедры от 21.06.19 № 16)

Заведующий кафедрой

С.Л. Зефирков

Работа защищена с отметкой

хорошо

(протокол заседания ГЭК

от 26.06.19 № 27)

Секретарь ГЭК

А.П. Иванов

Пенза 2019

Проверка ВКР – 9 баллов
 С.Л. Зефирков

Оглавление

Введение.....	6
1 Описание системы электронного документооборота и делопроизводства Пензенской области.....	8
1.1 Общее описание системы.....	8
1.2 Описание технологии обработки информации.....	9
1.3 Структура системы.....	11
2 Определение информации, подлежащей защите в системе электронного документооборота и делопроизводства Пензенской области.....	14
3 Определение перечня актуальных угроз безопасности информации.....	16
4 Классификация системы электронного документооборота и делопроизводства Пензенской области по требованиям защиты информации.....	35
4.1 Общая классификация системы.....	35
4.2 Определение требуемого уровня защищенности персональных данных.....	36
4.3 Определение класса защищенности информационной системы.....	37
5 Определение требований к системе защиты информации системы электронного документооборота и делопроизводства Пензенской области.....	39
6 Создание проекта системы защиты информации системы электронного документооборота и делопроизводства Пензенской области.....	70
6.1 Обоснование и выбор организационных мер по защите информации.....	70
6.2 Обоснование и выбор технических решений по защите информации.....	72
6.3 Определение мест размещения средств защиты информации.....	83
6.4 Создание проекта системы защиты.....	86
6.5 Разработка порядка и этапов внедрения системы защиты системы электронного документооборота и делопроизводства Пензенской области.....	

области.....	87
7 Вредные психофизиологические факторы, влияющие на опорно- двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	89
Заключение.....	91
Список используемых источников.....	92
Приложение А Проект системы защиты системы электронного документооборота и делопроизводства Пензенской области.....	97

Обозначения и сокращения

АПКШ – аппаратно-программный комплекс шифрования;
АРМ – автоматизированное рабочее место;
АС – аппаратное средство;
БИ – безопасность информации;
ВКР – выпускная квалификационная работа;
ГИС – государственная информационная система;
ИБ – информационная безопасность;
ИС – информационная система;
ИСПДн – информационная система персональных данных;
ИТКС – информационно-телекоммуникационная система;
МНИ – машинный носитель информации;
НПА – нормативно-правовой акт
НДВ – недекларированные возможности;
НСД – несанкционированный доступ;
ОГВ – органы государственной власти;
ОИВ – органы исполнительной власти;
ОМСУ – органы местного самоуправления;
ОРД – организационно-распорядительный документ;
ОС – операционная система;
ПДн – персональные данные;
ПО – программное обеспечение;
ПП – постановление Правительства;
ПЭМИН – побочные электромагнитные излучения и наводки;
РФ – Российская Федерация;
СЗИ – средство защиты информации;
СКЗИ – средство криптографической защиты информации;

СЭДД – система электронного документооборота и делопроизводства Пензенской области;

СФ – среда функционирования;

ТС – техническое средство;

ФАПСИ – Федеральное агентство правительственной связи и информации;

ФСБ – Федеральная служба безопасности;

ФСТЭК – Федеральная служба по техническому и экспортному контролю.

Введение

С развитием информационных технологий в современном мире наблюдается тенденция к автоматизации всех сфер деятельности человека. Одной из таких сфер является ведение документооборота. Для этого повсеместно внедряются системы электронного документооборота. Это позволяет добиться значительных результатов: уменьшить количество бумажных документов, снизить расходы на печать, канцтовары, отправку документов, значительно сократить трудозатраты на содержание архивов, а также обезопаситься от потерь документов и необходимости их восстановления в случае утраты.

При этом, наряду с преимуществами, проявляются и недостатки внедрения систем электронного документооборота, такие как новые риски, связанные с защитой сведений, обработка которых ведется в таких системах. Нарушение свойств конфиденциальности, целостности и доступности информации может нанести значительный ущерб организации вплоть до невозможности выполнения ею своих функций. При этом, кроме самих сведений, защите подлежат также носители данных, программные и аппаратные средства их обработки и линии связи. Для этого необходимо применение комплекса защитных мер, обеспечивающих защиту на всех уровнях, начиная от носителей информации и заканчивая организацией обработки данных.

В целях обеспечения безопасности сведений на территории Российской Федерации действует множество нормативно-правовых актов, регулирующих данную сферу деятельности. В частности, значительное число требований предъявляется к информационным системам, в которых ведется обработка персональных данных, а также к государственным информационным системам.

В число таких систем входит Система электронного документооборота и делопроизводства Пензенской области. Данная система обеспечивает работу органов государственной, исполнительной власти и органов местного

самоуправления Пензенской области, что предполагает обработку информации ограниченного доступа, в том числе персональных данных граждан. Соответственно, возникает необходимость защиты указанных сведений, для чего требуется построение системы защиты информации, удовлетворяющей требованиям нормативно-правовых актов, действующих на территории Российской Федерации.

1 Описание системы электронного документооборота и делопроизводства Пензенской области

1.1 Общее описание системы

Система электронного документооборота и делопроизводства Пензенской области (СЭДД) – это система, автоматизирующая управленческий документооборот и процессы делопроизводства в Правительстве Пензенской области, исполнительных органах государственной власти и органах местного самоуправления Пензенской области.

Система выполняет следующие задачи:

- регистрация и учет следующих видов документов:
 - входящей и исходящей корреспонденции;
 - внутренних документов (поручения, служебные и докладные записки, прочие документы);
 - постановлений и распоряжений Губернатора;
 - постановлений и распоряжений Правительства;
- контроль исполнения документов;
- поиск документов;
- хранение документов.

Для выполнения перечисленных задач в системе ведется обработка следующий видов документов:

- внутренние документы:
 - служебные и докладные записки;
 - статьи в печатных изданиях, книги, на которые наложена резолюция;
- информационные материалы;
- поручения, не связанные с документами;
- входящие документы:
 - письмо;

- факс;
- телеграмма;
- электронная почта;
- исходящие документы:
 - письма;
 - инициативные письма;
 - факсы;
 - телеграммы;
- обращения граждан.

Обрабатываемые в системе сведения могут содержать, в том числе, персональные данные сотрудников и граждан.

1.2 Описание технологии обработки информации

При работе пользователями создаются формы документов, для отражения информации по документу заполняются поля формы, присоединяются документы в формате MS Word, MS Excel или сканированные образы документов в формате PDF.

В системе ведется обработка следующих видов документов:

- входящие документы;
- исходящие документы;
- внутренние документы;
- организационно-распорядительные документы.

Входящие и внутренние документы проходят следующие этапы:

- регистрация. Входящие документы автоматически нумеруются средствами СЭДД. Документы регистрируются в СЭДД сотрудниками Канцелярии (входящие документы) или сотрудниками соответствующих приемных руководителей, секретариатов руководителей, наложивших резолюции (внутренние документы);

— маршрутизация. После регистрации электронные образы документов передаются назначенным лицам, ответственным за исполнение. К документу имеют доступ только делопроизводители и назначенные лица, ответственные за исполнение;

— наложение резолюции. Документы направляются руководителю. Руководитель (и лицо, его замещающее) имеет доступ только к тем входящим документам, которые адресованы непосредственно ему. После рассмотрения документа руководитель может наложить на него резолюцию, а также определить срок ее исполнения, ответственного исполнителя и соисполнителей. Регистрация резолюции осуществляется сотрудниками соответствующих приемных (секретариатов) руководителей;

— исполнение документа и наложенных на него резолюций. Исполнение документа осуществляется в порядке, предусмотренном Инструкцией по делопроизводству в аппарате Правительства. Когда резолюция исполнена, сотрудник соответствующей приемной (секретариата) делает отметку «Исполнено» и указывает дату исполнения. При этом автоматически будет создан отчет об исполнении;

— контроль за исполнение и снятие документа с контроля. Контроль за исполнением резолюции и снятие ее с контроля в СЭДД осуществляют сотрудники приемных, секретариатов, в которых данная резолюция была зарегистрирована. Отметка о снятии с контроля входящего в СЭДД документа осуществляется сотрудниками канцелярии после того, как сняты с контроля все резолюции, наложенные на него, и документ относится к делу. Внутренние документы снимаются с контроля сотрудниками приемной руководителя.

При работе с исходящими документами в СЭДД осуществляется их регистрация, а также постановка и снятие с контроля отдельных типов исходящих документов.

Исходящие документы подразделяются на письма, инициативные письма, факсы и телеграммы. Им также автоматически присваиваются номера.

Контролю исполнения подлежат только инициативные письма. Контроль исполнения инициативных писем осуществляет отдел по учету исполнения служебных документов. Как только документ исполнен, информация об этом передается сотрудниками отдела в канцелярию, где документ снимается с контроля в СЭДД.

Под организационно-распорядительными документами (ОРД) в данном подразумеваются постановления и распоряжения Губернатора Пензенской области, постановления и распоряжения Правительства Пензенской области, поручения на еженедельных оперативных совещаниях у Губернатора Пензенской области.

ОРД проходят следующие этапы:

- регистрация. ОРД и правовые акты Правительства регистрируются в протокольной части отдела делопроизводства Правительства Пензенской области;

- рассылка. Для рассылки ОРД ответственный сотрудник протокольной части отмечает его получателей согласно списку рассылки. Далее СЭДД автоматически осуществляет рассылку ОРД исполнителям;

- постановка на контроль и контроль за исполнением. На этом этапе доступ к ОРД получает отдел по учету исполнения служебных документов. Отдел по учету исполнения служебных документов осуществляет постановку на контроль, определение сроков исполнения документа;

- снятие с контроля. В СЭДД снятие с контроля ОРД осуществляет отдел по учету исполнения служебных документов, ответственные сотрудники которого вносят отметку о снятии с контроля.

1.3 Структура системы

Общая структура СЭДД представлена на рисунке 1.

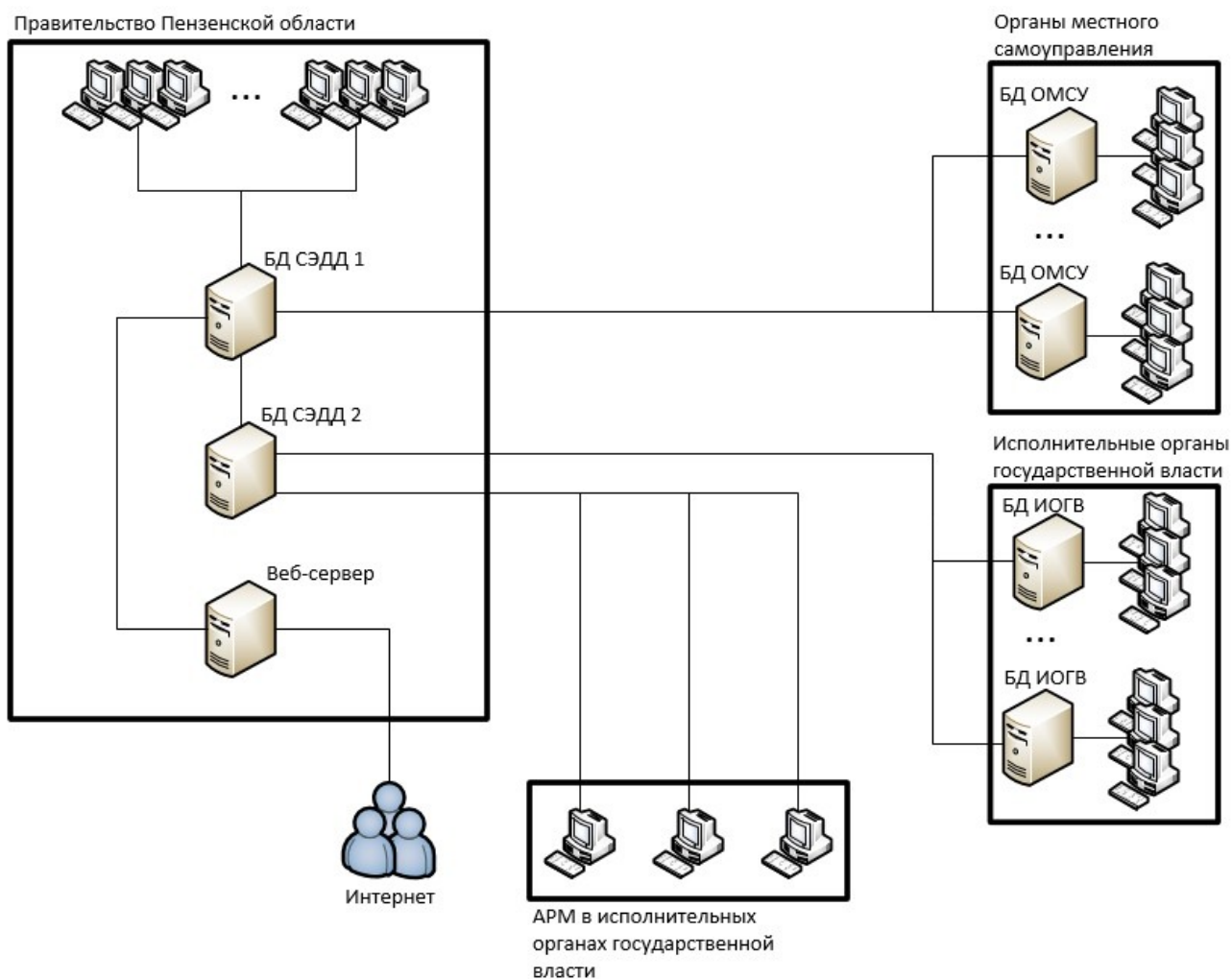


Рисунок 1 – Общая структура СЭДД

Основные базы данных системы электронного документооборота и делопроизводства Пензенской области, на которые реплицируются все другие базы данных СЭДД, размещаются в здании Правительства Пензенской области.

К СЭДД подключены все ОИВ и все ОМСУ Пензенской области.

В органах местного самоуправления Пензенской области и исполнительных органах государственной власти могут быть установлены свои сервера. В таком случае внутренний документооборот осуществляется без передачи информации на основные сервера.

Подключение к системе может осуществляться непосредственно с рабочих мест при помощи толстого или тонкого клиента СЭДД.

Кроме того, в систему заносятся обращения граждан. Регистрацию письменных обращений и обращений, присылаемых на электронную почту, осуществляют сотрудники канцелярии. Также существует возможность заполнения обращений на сайтах ОИВ и ОМСУ. Так как физически сервера органов власти расположены в здании Правительства, данные обращения попадают непосредственно на основные сервера СЭДД, а оттуда, при необходимости, маршрутизируются в отдельные органы власти.

Для обеспечения устойчивости системы используется процедура резервного копирования. Раз в день администратором выполняется полное резервное копирование всех баз данных СЭДД. При этом сроки хранения резервных копий следующие:

- ежедневные – 7 дней;
- ежемесячные – 1 год;
- годовая резервная копия переписывается на диск постоянного хранения.

2 Определение информации, подлежащей защите в системе электронного документооборота и делопроизводства Пензенской области

Для построения системы защиты информации в первую очередь необходимо определить информацию, подлежащую защите в соответствии с законодательством РФ. Для этого был использован «Перечень сведений конфиденциального характера», утвержденный указом Президента РФ от 6 марта 1997 г. № 188[4].

Во-первых, в системе ведется оборот документации, непосредственно связанной с деятельностью ОГВ, ОИВ и ОМСУ Пензенской области, а также документации, поступающей в систему от федеральных органов государственной власти. Однако в системе не обрабатываются сведения, составляющие служебную тайну. Таким образом, данные сведения не попадают ни под один пункт «Перечня сведений конфиденциального характера», утвержденного указом Президента РФ от 6 марта 1997 г. № 188[4].

Во-вторых, в систему заносятся и обрабатываются обращения граждан, заполняемые на сайтах органов государственной власти, органов исполнительной власти и органов местного самоуправления Пензенской области или направляемые в письменном виде. Данные сведения содержат персональные данные граждан, направивших обращение, которые могут быть отнесены к категории иных персональных данных, то есть не относящихся к категориям общедоступных, биометрических или специальных в соответствии с ФЗ РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»[5].

В-третьих, в системе обрабатываются персональные данные сотрудников, являющиеся общедоступными на основании трудового договора.

Перечень содержащихся в системе персональных данных представлен в таблице 1.

Таблица 1 – Перечень обрабатываемых в системе персональных данных

Содержание ПДн	Цели обработки ПДн	Основание для обработки ПДн	Категория ПДн
1. Персональные данные субъектов, являющихся сотрудниками оператора			
Фамилия, имя, отчество	Ведение делопроизводства, осуществление профессиональной деятельности	Трудовой договор с работником	Общедоступные ПДн
Должность	Ведение делопроизводства, осуществление профессиональной деятельности	Трудовой договор с работником	Общедоступные ПДн
Номер телефона	Ведение делопроизводства, осуществление профессиональной деятельности	Трудовой договор с работником	Общедоступные ПДн
2. Персональные данные субъектов, не являющихся сотрудниками оператора			
Фамилия, имя, отчество	Рассмотрение обращений граждан	ФЗ № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»	Иные ПДн
Адрес, по которому должен быть направлен ответ	Рассмотрение обращений граждан	ФЗ № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»	Иные ПДн
Телефон	Рассмотрение обращений граждан	ФЗ № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»	Иные ПДн

3 Определение перечня актуальных угроз безопасности информации

Для дальнейшей классификации информационной системы по требованиям защиты информации и построения системы защиты информации были определены угрозы, реализация которых может привести к нарушению БИ в ИС.

Для определения общего (предварительного) перечня угроз был использован Банк данных угроз безопасности информации ФСТЭК России[6]. Перечень определенных угроз безопасности информации представлен в таблице 3.

Таблица 3 – Перечень общих угроз безопасности информации

№	Код	Угроза
1	УБИ.004	Угроза аппаратного сброса пароля BIOS
2	УБИ.005	Угроза внедрения вредоносного кода в BIOS
3	УБИ.006	Угроза внедрения кода или данных
4	УБИ.008	Угроза восстановления аутентификационной информации
5	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
6	УБИ.018	Угроза загрузки нештатной операционной системы
7	УБИ.023	Угроза изменения компонентов системы
8	УБИ.030	Угроза использования информации идентификации / аутентификации, заданной по умолчанию
9	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
10	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
11	УБИ.069	Угроза неправомерных действий в каналах связи
12	УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
13	УБИ.088	Угроза несанкционированного копирования защищаемой информации
14	УБИ.090	Угроза несанкционированного создания учётной записи пользователя
15	УБИ.091	Угроза несанкционированного удаления защищаемой информации

Продолжение таблицы 3

№	Код	Угроза
16	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
17	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
18	УБИ.139	Угроза преодоления физической защиты
19	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
20	УБИ.156	Угроза утраты носителей информации
21	УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
22	УБИ.158	Угроза форматирования носителей информации
23	УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
24	УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
25	УБИ.172	Угроза распространения «почтовых червей»
26	УБИ.179	Угроза несанкционированной модификации защищаемой информации
27	УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
28	УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет
29	УБИ.192	Угроза использования уязвимых версий программного обеспечения

Также с использованием БДУ ФСТЭК[7] были выявлены уязвимости, эксплуатация которых возможна при реализации угроз БИ. Перечень уязвимостей представлен в таблице 4.

Таблица 4 – Перечень уязвимостей, которые могут быть использованы для реализации угроз БИ

№	Угроза	Уязвимости
1	Угроза аппаратного сброса пароля BIOS	Слабость контроля доступа лиц в контролируемой зоне
2	Угроза внедрения вредоносного кода в BIOS	Слабость контроля доступа лиц в контролируемой зоне

Продолжение таблицы 4

№	Угроза	Уязвимости
3	Угроза внедрения кода или данных	Слабость мер антивирусной защиты
4	Угроза восстановления аутентификационной информации	Слабость парольной политики
5	Угроза восстановления предыдущей уязвимой версии BIOS	Слабость контроля за обновлением программного обеспечения
6	Угроза загрузки нештатной операционной системы	Слабость технологий разграничения доступа к управлению BIOS/UEFI
7	Угроза изменения компонентов системы	Слабость мер контроля за целостностью аппаратной конфигурации информационной системы
8	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Слабость парольной политики
9	Угроза использования слабостей протоколов сетевого/локального обмена данными	Наличие слабостей в протоколах сетевого/локального обмена данными
10	Угроза неправомерного ознакомления с защищаемой информацией	Ошибки в параметрах конфигурации средств контроля доступа
11	Угроза неправомерных действий в каналах связи	Наличие слабостей в протоколах сетевого/локального обмена данными
12	Угроза несанкционированного использования привилегированных функций BIOS	Слабость мер разграничения доступа к функционалу BIOS
13	Угроза несанкционированного копирования защищаемой информации	Слабость механизмов разграничения доступа к защищаемой информации
		Слабость контроля доступа лиц в контролируемой зоне
14	Угроза несанкционированного создания учётной записи пользователя	Слабость механизмов разграничения доступа к защищаемой информации
15	Угроза несанкционированного удаления защищаемой информации	Слабость механизмов разграничения доступа к защищаемой информации
		Слабость контроля доступа лиц в контролируемой зоне
16	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Слабости механизмов разграничения доступа, предоставляющие нарушителю привелегии на установку и запуск специализированных вредоносных программ

Продолжение таблицы 4

№	Угроза	Уязвимости
17	Угроза перехвата данных, передаваемых по вычислительной сети	Слабости механизмов сетевого взаимодействия, предоставляющие сторонним пользователям открытые данные о дискредитируемой системе
18	Угроза преодоления физической защиты	Уязвимости в системе контроля физического доступа
19	Угроза приведения системы в состояние «отказ в обслуживании»	Недостаточность мер контроля за управлением соединениями
20	Угроза утраты носителей информации	Слабости мер регистрации и учета носителей информации
21	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Слабость мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации
22	Угроза форматирования носителей информации	Слабость мер ограничения доступа к системной функции форматирования носителей информации
23	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Слабость мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации
24	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Слабость механизмов фильтрации сетевого трафика Слабость мер антивирусного контроля
25	Угроза распространения «почтовых червей» сайтов в сети Интернет	Слабость мер антивирусного контроля
26	Угроза несанкционированной модификации защищаемой информации	Слабость механизмов разграничения доступа к защищаемой информации Слабость контроля доступа лиц в контролируемой зоне
27	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Слабость механизмов фильтрации сетевого трафика Слабость мер антивирусного контроля
28	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Слабость мер антивирусной защиты Отсутствие правил межсетевого экранирования

Продолжение таблицы 4

№	Угроза	Уязвимости
29	Угроза использования уязвимых версий программного обеспечения	Слабость контроля за обновлением программного обеспечения

Далее был определен перечень возможных нарушителей, представленный в таблице 5. Для этого была использована «Методика определения угроз безопасности информации в информационных системах» ФСТЭК России[7].

Таблица 5 – Перечень возможных нарушителей

№	Вид нарушителя	Тип нарушителя	Потенциал нарушителя	Мотивация нарушителя
1	Преступные группы (криминальные структуры)	Внешний	Средний	Причинение имущественного ущерба путем мошенничества или иным преступным путем; выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.
2	Внешние субъекты (физические лица)	Внешний	Низкий	Идеологические или политические мотивы; причинение имущественного ущерба путем мошенничества или иным преступным путем; любопытство или желание самореализации (подтверждение статуса); выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.
3	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;	Внутренний	Низкий	Причинение имущественного ущерба путем обмана или злоупотребления доверием; непреднамеренные, неосторожные или неквалифицированные действия.

Продолжение таблицы 5

№	Вид нарушителя	Тип нарушителя	Потенциал нарушителя	Мотивация нарушителя
4	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Низкий	Причинение имущественного ущерба путем обмана или злоупотребления доверием; непреднамеренные, неосторожные или неквалифицированные действия.
5	Пользователи информационной системы	Внутренний	Низкий	Причинение имущественного ущерба путем мошенничества или иным преступным путем; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия; непреднамеренные, неосторожные или неквалифицированные действия.
6	Администраторы информационной системы и администраторы безопасности	Внутренний	Средний	Причинение имущественного ущерба путем мошенничества или иным преступным путем; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия; выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды; непреднамеренные, неосторожные или неквалифицированные действия.
7	Бывшие работники (пользователи)	Внешний	Низкий	Причинение имущественного ущерба путем мошенничества или иным преступным путем; месть за ранее совершенные действия.

Так как система является распределенной, для нейтрализации угроз необходимо использование СКЗИ. При этом, в соответствии с приказом ФСБ РФ №387, необходимо «формирование совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак»[8].

Обобщенные возможности источников атак представлены в таблице 6.

Таблица 6 – Обобщенные возможности источников атак

№	Обобщенные возможности источников атак	Да/нет
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах КЗ, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования (далее – СФ)	Нет
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах КЗ с физическим доступом к АС, на которых реализованы СКЗИ и их СФ	Нет
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов ПЭМИН СКЗИ)	Нет
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак НДВ прикладного ПО)	Нет
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак НДВ аппаратного и программного компонентов СФ СКЗИ)	Нет

Уточненные возможности источников атак представлены в таблице 7.

Таблица 7 – Уточненные возможности источников атак

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	Проведение атаки при нахождении в пределах КЗ	Неактуально	доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода.
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ.	Неактуально	доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода.
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:	Актуально	—

Продолжение таблицы 7

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	<ul style="list-style-type: none"> - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ. 		
1.4	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	Неактуально	Осуществляется регистрация и учет действий пользователей; в ИСПДн используются: сертифицированные средства защиты информации от несанкционированного доступа; сертифицированные средства антивирусной защиты.
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ.	Неактуально	доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода.
2.2	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в ИС, в которой используется	Неактуально	Проводятся работы по подбору персонала; представители технических, обслуживающих и других вспомогательных служб при

Продолжение таблицы 7

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.		работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации.
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак НДВ прикладного ПО.	Неактуально	Не осуществляется обработка ССГТ, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченные мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	Неактуально	Не осуществляется обработка ССГТ, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
3.3	Проведение работ по созданию способов и средств атак в научно - исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.	Неактуально	Не осуществляется обработка ССГТ, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.

Продолжение таблицы 7

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак НДВ системного ПО.	Неактуально	Не осуществляется обработка ССГТ, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.	Неактуально	Не осуществляется обработка ССГТ, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ.	Неактуально	Не осуществляется обработка ССГТ, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.

Затем с использованием «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России[9] была определена актуальность выявленных угроз.

Изначально был определен уровень исходной защищенности СЭДД, как представлено в таблице 8.

Таблица 8 – Определение уровня исходной защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
<p>1. По территориальному размещению:</p> <p>распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;</p>	-	-	+
<p>2. По наличию соединения с сетями общего пользования:</p> <p>ИСПДн, имеющая многоточечный выход в сеть общего пользования;</p>	-	-	+
<p>3. По встроенным (легальным) операциям с записями баз персональных данных:</p> <p>запись, удаление, сортировка;</p>	-	+	-
<p>4. По разграничению доступа к персональным данным:</p> <p>ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;</p>	-	+	-
<p>5. По наличию соединений с другими базами ПДн иных ИСПДн:</p> <p>интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);</p>	-	-	+

Продолжение таблицы 8

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
5. По наличию соединений с другими базами ПДн иных ИСПДн: интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	-	-	+
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	-	+	-
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, не предоставляющая никакой информации.	+	-	-

Так как высокому и среднему уровням защищенности соответствуют только 57% показателей, система имеет низкий уровень защищенности.

Далее были определены вероятность (частота) и возможность реализации каждой угрозы. Результат представлен в таблице 9.

Таблица 9 – Определение вероятности (частоты) и возможности реализации угроз БИ

Угроза	Степень исходной защищенности	Вероятность реализации угрозы	Возможность реализации угрозы
Угроза аппаратного сброса пароля BIOS	Низкая	Низкая	Средняя
Угроза внедрения вредоносного кода в BIOS	Низкая	Низкая	Средняя
Угроза внедрения кода или данных	Низкая	Средняя	Высокая
Угроза восстановления аутентификационной информации	Низкая	Средняя	Высокая
Угроза восстановления предыдущей уязвимой версии BIOS	Низкая	Низкая	Средняя
Угроза загрузки нештатной операционной системы	Низкая	Высокая	Очень высокая
Угроза изменения компонентов системы	Низкая	Высокая	Очень высокая
Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Низкая	Низкая	Средняя
Угроза использования слабостей протоколов сетевого/локального обмена данными	Низкая	Низкая	Средняя
Угроза неправомерного ознакомления с защищаемой информацией	Низкая	Высокая	Очень высокая
Угроза неправомерных действий в каналах связи	Низкая	Низкая	Средняя
Угроза несанкционированного использования привилегированных функций BIOS	Низкая	Низкая	Средняя
Угроза несанкционированного копирования защищаемой информации	Низкая	Высокая	Очень высокая
Угроза несанкционированного создания учётной записи пользователя	Низкая	Низкая	Средняя
Угроза несанкционированного удаления защищаемой информации	Низкая	Средняя	Высокая
Угроза перехвата вводимой и выводимой на периферийные устройства информации	Низкая	Средняя	Высокая

Продолжение таблицы 9

Угроза	Степень исходной защищенности	Вероятность реализации угрозы	Возможность реализации угрозы
Угроза перехвата данных, передаваемых по вычислительной сети	Низкая	Высокая	Очень высокая
Угроза преодоления физической защиты	Низкая	Низкая	Средняя
Угроза приведения системы в состояние «отказ в обслуживании»	Низкая	Низкая	Средняя
Угроза утраты носителей информации	Низкая	Средняя	Высокая
Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Низкая	Низкая	Средняя
Угроза форматирования носителей информации	Низкая	Низкая	Средняя
Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Низкая	Средняя	Высокая
Угроза заражения компьютера при посещении неблагонадёжных сайтов	Низкая	Низкая	Средняя
Угроза распространения «почтовых червей» сайтов в сети Интернет	Низкая	Низкая	Средняя
Угроза несанкционированной модификации защищаемой информации	Низкая	Средняя	Высокая
Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Низкая	Низкая	Средняя
Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Низкая	Низкая	Средняя
Угроза использования уязвимых версий программного обеспечения	Низкая	Средняя	Высокая

Далее была определена актуальность угроз в соответствии с правилами, приведенными в таблице 10.

Таблица 10 – Правила отнесения угрозы БИ к актуальной

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

Определение актуальности каждой из угроз представлено в таблице 11.

Таблица 11 – Определение актуальности угроз БИ

Угроза	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
Угроза аппаратного сброса пароля BIOS	Средняя	Низкий	Неактуальная
Угроза внедрения вредоносного кода в BIOS	Средняя	Низкий	Неактуальная
Угроза внедрения кода или данных	Средняя	Средний	Актуальная
Угроза восстановления аутентификационной информации	Высокая	Средний	Актуальная
Угроза восстановления предыдущей уязвимой версии BIOS	Средняя	Низкий	Неактуальная
Угроза загрузки нештатной операционной системы	Очень высокая	Низкий	Актуальная
Угроза изменения компонентов системы	Очень высокая	Средний	Актуальная
Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Средняя	Средний	Актуальная
Угроза использования слабостей протоколов сетевого/локального обмена данными	Средняя	Средний	Актуальная
Угроза неправомерного ознакомления с защищаемой информацией	Средняя	Средний	Актуальная

Продолжение таблицы 11

Угроза	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
Угроза неправомерных действий в каналах связи	Средняя	Низкий	Неактуальная
Угроза несанкционированного использования привилегированных функций BIOS	Средняя	Низкий	Неактуальная
Угроза несанкционированного копирования защищаемой информации	Высокая	Средний	Актуальная
Угроза несанкционированного создания учётной записи пользователя	Средняя	Средний	Актуальная
Угроза несанкционированного удаления защищаемой информации	Высокая	Средний	Актуальная
Угроза перехвата вводимой и выводимой на периферийные устройства информации	Высокая	Средний	Актуальная
Угроза перехвата данных, передаваемых по вычислительной сети	Очень высокая	Средний	Актуальная
Угроза преодоления физической защиты	Средняя	Средний	Актуальная
Угроза приведения системы в состояние «отказ в обслуживании»	Средняя	Средний	Актуальная
Угроза утраты носителей информации	Высокая	Средний	Актуальная
Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Средняя	Низкий	Неактуальная
Угроза форматирования носителей информации	Средняя	Средний	Актуальная

Продолжение таблицы 11

Угроза	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность
Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Высокая	Средний	Актуальная
Угроза заражения компьютера при посещении неблагонадёжных сайтов	Средняя	Средний	Актуальная
Угроза распространения «почтовых червей» сайтов в сети Интернет	Средняя	Средний	Актуальная
Угроза несанкционированной модификации защищаемой информации	Высокая	Средний	Актуальная
Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Средняя	Средний	Актуальная
Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Средняя	Средний	Актуальная
Угроза использования уязвимых версий программного обеспечения	Высокая	Низкий	Актуальная

Для классификации СЭДД по требованиям защиты информации для актуальных угроз были определены их типы на основании ПП РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[10]. Итоговый перечень актуальных угроз с указанием их типа представлен в таблице 12.

Таблица 12 – Перечень актуальных угроз с указанием их типа

№	Угроза	Тип угрозы
1	Угроза внедрения кода или данных	3 тип
2	Угроза восстановления аутентификационной информации	3 тип
3	Угроза загрузки нештатной операционной системы	3 тип
4	Угроза изменения компонентов системы	3 тип

Продолжение таблицы 12

№	Угроза	Тип угрозы
5	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	3 тип
6	Угроза использования слабостей протоколов сетевого/локального обмена данными	3 тип
7	Угроза неправомерного ознакомления с защищаемой информацией	3 тип
8	Угроза несанкционированного копирования защищаемой информации	3 тип
9	Угроза несанкционированного создания учётной записи пользователя	3 тип
10	Угроза несанкционированного удаления защищаемой информации	3 тип
11	Угроза перехвата вводимой и выводимой на периферийные устройства информации	3 тип
12	Угроза перехвата данных, передаваемых по вычислительной сети	3 тип
13	Угроза преодоления физической защиты	3 тип
14	Угроза приведения системы в состояние «отказ в обслуживании»	3 тип
15	Угроза утраты носителей информации	3 тип
16	Угроза форматирования носителей информации	3 тип
17	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	3 тип
18	Угроза заражения компьютера при посещении неблагонадёжных сайтов	3 тип
19	Угроза распространения «почтовых червей» сайтов в сети Интернет	3 тип
20	Угроза несанкционированной модификации защищаемой информации	3 тип
21	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	3 тип
22	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	3 тип
23	Угроза использования уязвимых версий программного обеспечения	3 тип

4 Классификация системы электронного документооборота и делопроизводства Пензенской области по требованиям защиты информации

4.1 Общая классификация системы

Классификация системы была осуществлена на основе определенной в п. 3 информации, подлежащей защите в системе электронного документооборота и делопроизводства Пензенской области.

Так как в СЭДД ведется обработка персональных данных, система является информационной системой персональных данных.

Определение государственных информационных систем приведено в ФЗ от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»[11].

В соответствии со статьей 13 «государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов»[11].

СЭДД Пензенской области является региональной информационной системой и введена в эксплуатацию Распоряжением Правительства Пензенской области. Данный документ является правовым актом государственного органа.

В статье 14 ФЗ от 27.07.2006 № 149-ФЗ указано, что «Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях»[11]. Целью создания СЭДД является обеспечение обмена информацией между ОГВ, ОИВ и ОМСУ Пензенской области.

На основании вышеизложенного можно сделать вывод, что СЭДД является государственной информационной системой.

4.2 Определение требуемого уровня защищенности персональных данных

Для защиты информации в ИСПДн изначально следует определить уровень защищенности персональных данных. Критерии определения уровня защищенности приведены в Постановлении Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[10].

Было проведено исследование рассматриваемой системы и определены исходные данные для определения уровня защищенности ПДн. Результаты представлены в таблице 13.

Таблица 13 – Исходные показатели ИСПДн для определения требуемого уровня защищенности персональных данных

№	Условия обработки персональных данных	Показатель
1	Категории обрабатываемых персональных данных	Общедоступные, иные
2	Категории субъектов	Являющиеся сотрудниками оператора, не являющиеся сотрудниками оператора
3	Количество субъектов, не являющихся сотрудниками оператора	Более 100 000
4	Тип актуальных угроз	3 тип

В соответствие с ПП РФ от 01.11.2012 № 1119 в информационной системе необходимо обеспечение 3 уровня защищенности ПДн.

В соответствии с ПП РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» «Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как

использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.»[12] На основании исследования информационных процессов, протекающих в системе, можно сделать вывод о том, что обработка ПДн осуществляется без использования средств автоматизации.

4.3 Определение класса защищенности информационной системы

Определение класса защищенности ГИС осуществляется на основании приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[13].

Масштаб ИС – региональный, так как СЭДД функционирует на территории субъекта Российской Федерации и имеет сегменты в нескольких муниципальных образованиях и подведомственных и иных организациях.

Уровень значимости информации – низкий, так как нарушение безопасности информации в системе может быть причиной незначительных негативных последствий в социальной, политической, международной, экономической, финансовой или иных областях деятельности, и выполнение своих функций органами государственной и исполнительной власти, а также органами местного самоуправления возможно, но с недостаточной эффективностью или с привлечением дополнительных сил и средств.

На представленных выше сведениях можно сделать вывод, что СЭДД имеет класс защищенности КЗ.

Так как в системе ведется обработка персональных данных, требуется согласование уровня защищенности персональных данных и класса защищенности информационной системы. Из приказа ФСТЭК России от 11 февраля 2013 г. № 17 «для информационной системы 3 класса защищенности

обеспечивают 3 и 4 уровни защищенности персональных данных»[13]. Следовательно, для выполнения требования нет необходимости изменять уровень защищенности ПДн или класс защищенности информационной системы.

5 Определение требований к системе защиты информации системы электронного документооборота и делопроизводства Пензенской области

По результатам выполненной классификации был определен перечень требований, предъявляемых к системе защиты информации СЭДД.

В первую очередь, требуется выполнение приказов ФСТЭК России от 11 февраля 2013 г. №17[13].

Сначала были определены меры, необходимые для обеспечения 3 класса защищенности ГИС. Базовый набор мер представлен в приказе ФСТЭК России №17[13].

Затем была проведена адаптация базового набора. Обоснование включения мер базового набора в адаптированный представлено в таблице 14.

Таблица 14 – Обоснование включения мер в адаптированный набор

Условные обозначения группы мер	Описание группы мер	Обоснование адаптации
ИАФ	Идентификация и аутентификация субъектов доступа и объектов доступа	Меры идентификации и аутентификации должны применяться, так как необходимо контролировать доступ всех пользователей к ресурсам системы, определять пользователей, которым доступ может быть предоставлен к отдельным компонентам системы и тех, которым доступ должен быть запрещен.
УПД	Управление доступом субъектов доступа к объектам доступа	Для реализации контроля доступа всех пользователей к ресурсам системы необходима реализация управления доступом субъектов к объектам.
ОПС	Ограничение программной среды	Реализация мер данной группы обусловлена необходимостью контроля устанавливаемого на средствах вычислительной техники ПО
ЗНИ	Защита машинных носителей персональных данных	Реализация мер данной группы необходима, так как возможна утечка защищаемой информации вследствие недостаточного контроля за носителями такой информации

Продолжение таблицы 14

Условные обозначения группы мер	Описание группы мер	Обоснование адаптации
РСБ	Регистрация событий безопасности	Реализация мер данной группы необходима для обеспечения возможности мониторинга событий ИБ, происходящих в системе, выявления инцидентов и оперативного реагирования на них, а также для выявления причин возникновения инцидентов
АВЗ	Антивирусная защита	Меры данной группы должны быть реализованы, так как антивирусная защита является наиболее эффективной для обеспечения защиты от внедрения в систему вредоносного кода
СОВ	Обнаружение вторжений	Реализация мер данной группы необходима для обеспечения возможности мониторинга информационных процессов, протекающих в системе и сигнализации об аномальных ситуациях, указывающих на реализацию угроз БИ
АНЗ	Контроль (анализ) защищенности персональных данных	Реализация мер данной группы необходима для выявления слабостей или нарушений в системе защиты информации и для их оперативного устранения
ОЦЛ	Обеспечение целостности информационной системы и персональных данных	Реализация мер данной группы необходима для защиты от несанкционированной модификации защищаемой информации, установленного в системе ПО и СЗИ, а также от внедрения в систему вредоносного ПО
ОДТ	Обеспечение доступности персональных данных	Реализация мер данной группы необходима для обеспечения непрерывного функционирования системы, а также для возможности восстановления защищаемой информации при ее потере в результате сбоев или несанкционированных действий нарушителей

Продолжение таблицы 14

Условные обозначения группы мер	Описание группы мер	Обоснование адаптации
ЗСВ	Защита среды виртуализации	Реализация мер данной группы не требуется, так как в системе не используются технологии виртуализации
ЗТС	Защита технических средств	Реализация мер данной группы необходима, так как исключение возможности доступа нарушителя к компонентам системы существенно затрудняет реализацию большинства угроз БИ
ЗИС	Защита ИС, ее средств, систем связи и передачи данных	Реализация мер данной группы необходима для защиты информации от ее раскрытия при передаче по каналам связи

Обоснование исключения мер из базового набора представлено в таблице 15.

Таблица 15 – Обоснование исключения мер из базового набора

Условное обозначение и номер мер	Содержание мер по обеспечению безопасности персональных данных	Обоснование исключения из базового набора
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Мера исключена, так как в системе работают только внутренние пользователи, являющиеся сотрудниками оператора
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Мера исключена, так как в ИСПДн не используются технологии беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Мера исключена, так как в системе не используются мобильные технические средства
ЗСВ.1, ЗСВ.2, ЗСВ.3, ЗСВ.9, ЗСВ.10	Защита среды виртуализации	Группа мер исключена, так как в системе не используется технология виртуализации

Продолжение таблицы 15

Условное обозначение и номер мер	Содержание мер по обеспечению безопасности персональных данных	Обоснование исключения из базового набора
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	Мера исключена, так как в системе не используются средства, которые могут активироваться удаленно
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Мера исключена, так как в системе не используется технология беспроводных соединений
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе	Мера исключена, так как в системе не используются мобильные технические средства

Таким образом, в адаптированный базовый набор были включены меры, представленные в таблице 16.

Таблица 16 – Защитные меры, включенные в адаптированный базовый набор

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	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление 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
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов, типов и правил разграничения доступа

Продолжение таблицы 16

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
УПД.3	Управление информационными потоками между устройствами, сегментами ИС, а также между информационными системами
УПД.4	Разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование ИС
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС
УПД.6	Ограничение неуспешных попыток входа в ИС
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия 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 ИТКС
УПД.16	Управление взаимодействием с ИС сторонних организаций
III. Ограничение программной среды (ОПС)	
ОПС.3	Установка только разрешенного к использованию ПО и (или) его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет МНИ
ЗНИ.2	Управление доступом к МНИ
ЗНИ.8	Уничтожение информации на МНИ при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения
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.3	Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

Продолжение таблицы 16

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
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)
VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений ПО, включая обновление ПО СЗИ
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ
АНЗ.4	Контроль состава ТС, ПО и СЗИ
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)	
ОЦЛ.3	Обеспечение возможности восстановления ПО, включая ПО СЗИ, при возникновении нештатных ситуаций
XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные ТС, обрабатывающие информацию, и СЗИ, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к ТС, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам ЗИ и средствам обеспечения функционирования ИС и помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение ЗИ от раскрытия, модификации и навязывания при ее передаче по каналам связи, имеющим выход за пределы КЗ, в том числе беспроводным каналам связи

Для уточнения адаптированного набора мер было проведено соотнесение защитных мер из адаптированного набора и актуальных угроз БИ, а затем соотнесение актуальных угроз и нейтрализующих их защитных мер.

Результат соотнесения защитных мер и угроз представлен в таблице 17.

Таблица 17 – Соотнесения защитных мер и угроз

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Угроза неправомерного ознакомления с защищаемой информацией; Угроза несанкционированного копирования защищаемой информации; Угроза несанкционированного удаления защищаемой информации; Угроза несанкционированной модификации защищаемой информации
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Угроза несанкционированного создания учётной записи пользователя
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Угроза восстановления аутентификационной информации; Угроза использования информации идентификации/аутентификации, заданной по умолчанию
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Угроза восстановления аутентификационной информации
II. Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Управление учетными записями пользователей, в том числе внешних пользователей	Угроза неправомерного ознакомления с защищаемой информацией; Угроза несанкционированного копирования защищаемой информации; Угроза несанкционированного создания учётной записи пользователя;

Продолжение таблицы 17

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
		<p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза несанкционированной модификации защищаемой информации</p>
УПД.2	Реализация необходимых методов, типов и правил разграничения доступа	<p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза несанкционированной модификации защищаемой информации</p>
УПД.3	Управление информационными потоками между устройствами, сегментами ИС, а также между информационными системами	<p>Угроза использования слабостей протоколов сетевого/локального обмена данными;</p> <p>Угроза перехвата данных, передаваемых по вычислительной сети</p>
УПД.4	Разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование ИС	<p>Угроза внедрения кода или данных</p> <p>Угроза загрузки нештатной операционной системы</p> <p>Угроза неправомерного ознакомления с защищаемой информацией</p> <p>Угроза несанкционированного копирования защищаемой информации</p> <p>Угроза несанкционированного удаления защищаемой информации</p> <p>Угроза форматирования носителей информации</p> <p>Угроза несанкционированной модификации защищаемой информации</p>
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС	<p>Угроза внедрения кода или данных</p> <p>Угроза загрузки нештатной операционной системы</p>

Продолжение таблицы 17

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
		<p>Угроза неправомерного ознакомления с защищаемой информацией</p> <p>Угроза несанкционированного копирования защищаемой информации</p> <p>Угроза несанкционированного удаления защищаемой информации</p> <p>Угроза форматирования носителей информации</p> <p>Угроза несанкционированной модификации защищаемой информации</p>
УПД.6	Ограничение неуспешных попыток входа в ИС	Угроза восстановления аутентификационной информации
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия пользователя или по его запросу	<p>Угроза внедрения кода или данных;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза несанкционированной модификации защищаемой информации;</p>
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	<p>Угроза внедрения кода или данных</p> <p>Угроза загрузки нештатной операционной системы;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза несанкционированной модификации защищаемой информации</p>

Продолжение таблицы 17

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние ИТКС	<p>Угроза использования слабостей протоколов сетевого/локального обмена данными;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза несанкционированной модификации защищаемой информации</p>
УПД.16	Управление взаимодействием с ИС сторонних организаций	<p>Угроза внедрения кода или данных;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза несанкционированной модификации защищаемой информации</p>
III. Ограничение программной среды (ОПС)		
ОПС.3	Установка только разрешенного к использованию ПО и (или) его компонентов	<p>Угроза внедрения кода или данных;</p> <p>Угроза изменения компонентов системы;</p> <p>Угроза перехвата вводимой и выводимой на периферийные устройства информации;</p> <p>Угроза использования уязвимых версий программного обеспечения</p>
IV. Защита машинных носителей информации (ЗНИ)		
ЗНИ.1	Учет МНИ	<p>Угроза утраты носителей информации;</p> <p>Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации</p>

Продолжение таблицы 17

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
ЗНИ.2	Управление доступом к МНИ	<p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза несанкционированной модификации защищаемой информации.</p>
ЗНИ.8	Уничтожение информации на МНИ при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения	<p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации.</p>
V. Регистрация событий безопасности (РСБ)		
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	<p>Угроза внедрения кода или данных</p> <p>Угроза восстановления аутентификационной информации</p> <p>Угроза изменения компонентов системы</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного создания учётной записи пользователя;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза приведения системы в состояние «отказ в обслуживании»;</p>

Продолжение таблицы 17

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
		Угроза несанкционированной модификации защищаемой информации.
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	<p>Угроза внедрения кода или данных;</p> <p>Угроза восстановления аутентификационной информации;</p> <p>Угроза изменения компонентов системы;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного создания учётной записи пользователя;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза приведения системы в состояние «отказ в обслуживании»;</p> <p>Угроза несанкционированной модификации защищаемой информации.</p>
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения	<p>Угроза внедрения кода или данных;</p> <p>Угроза восстановления аутентификационной информации;</p> <p>Угроза изменения компонентов системы;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного создания учётной записи пользователя;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза приведения системы в состояние «отказ в обслуживании»;</p>

Продолжение таблицы 17

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
		Угроза несанкционированной модификации защищаемой информации.
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	<p>Угроза внедрения кода или данных;</p> <p>Угроза восстановления аутентификационной информации;</p> <p>Угроза изменения компонентов системы;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного создания учётной записи пользователя;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза приведения системы в состояние «отказ в обслуживании»;</p> <p>Угроза несанкционированной модификации защищаемой информации.</p>
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	<p>Угроза внедрения кода или данных;</p> <p>Угроза восстановления аутентификационной информации;</p> <p>Угроза изменения компонентов системы;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного создания учётной записи пользователя;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза приведения системы в состояние «отказ в обслуживании»;</p>

Продолжение таблицы 17

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
		Угроза несанкционированной модификации защищаемой информации.
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	Угроза внедрения кода или данных
РСБ.7	Защита информации о событиях безопасности	Угроза неправомерного ознакомления с защищаемой информацией; Угроза несанкционированного копирования защищаемой информации; Угроза несанкционированного удаления защищаемой информации; Угроза несанкционированной модификации защищаемой информации;
VI. Антивирусная защита (AB3)		
AB3.1	Реализация антивирусной защиты	Угроза внедрения кода или данных; Угроза перехвата вводимой и выводимой на периферийные устройства информации; Угроза приведения системы в состояние «отказ в обслуживании»; Угроза заражения компьютера при посещении неблагодёжных сайтов; Угроза распространения «почтовых червей» сайтов в сети Интернет; Угроза внедрения вредоносного кода через рекламу, сервисы и контент; Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет
AB3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Угроза внедрения кода или данных; Угроза перехвата вводимой и выводимой на периферийные устройства информации; Угроза приведения системы в состояние «отказ в обслуживании»; Угроза заражения компьютера при посещении неблагодёжных сайтов;

Продолжение таблицы 17

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
		<p>Угроза распространения «почтовых червей» сайтов в сети Интернет ;</p> <p>Угроза внедрения вредоносного кода через рекламу, сервисы и контент;</p> <p>Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет</p>
VIII. Контроль (анализ) защищенности информации (АНЗ)		
АНЗ.1	Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей	<p>Угроза внедрения кода или данных;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза приведения системы в состояние «отказ в обслуживании»;</p> <p>Угроза несанкционированной модификации защищаемой информации;</p> <p>Угроза использования уязвимых версий программного обеспечения</p>
АНЗ.2	Контроль установки обновлений ПО, включая обновление ПО СЗИ	Угроза использования уязвимых версий программного обеспечения
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ	<p>Угроза внедрения кода или данных;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза приведения системы в состояние «отказ в обслуживании»;</p> <p>Угроза несанкционированной модификации защищаемой информации</p>
АНЗ.4	Контроль состава ТС, ПО и СЗИ	Угроза изменения компонентов системы

Продолжение таблицы 17

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС	<p>Угроза восстановления аутентификационной информации;</p> <p>Угроза использования информации идентификации/аутентификации, заданной по умолчанию;</p> <p>Угроза неправомерного ознакомления с защищаемой информацией</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного создания учётной записи пользователя;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза несанкционированной модификации защищаемой информации</p>
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)		
ОЦЛ.3	Обеспечение возможности восстановления ПО, включая ПО СЗИ, при возникновении нештатных ситуаций	<p>Угроза изменения компонентов системы;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза несанкционированной модификации защищаемой информации;</p> <p>Угроза использования уязвимых версий программного обеспечения</p>
XII. Защита технических средств (ЗТС)		
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные ТС, обрабатывающие информацию, и СЗИ, а также средства обеспечения функционирования	<p>Угроза неправомерного ознакомления с защищаемой информацией;</p> <p>Угроза несанкционированного копирования защищаемой информации;</p> <p>Угроза несанкционированного удаления защищаемой информации;</p> <p>Угроза преодоления физической защиты;</p> <p>Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;</p>

Продолжение таблицы 17

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Нейтрализуемые угрозы
		Угроза несанкционированной модификации защищаемой информации
ЗТС.3	Контроль и управление физическим доступом к ТС, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключаящие несанкционированный физический доступ к средствам обработки информации, средствам ЗИ и средствам обеспечения функционирования ИС и помещения и сооружения, в которых они установлены	Угроза внедрения кода или данных; Угроза изменения компонентов системы; Угроза неправомерного ознакомления с защищаемой информацией; Угроза несанкционированного копирования защищаемой информации; Угроза несанкционированного удаления защищаемой информации; Угроза перехвата вводимой и выводимой на периферийные устройства информации; Угроза преодоления физической защиты; Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации; Угроза несанкционированной модификации защищаемой информации
ЗТС.4	Размещение устройств вывода информации, исключаящее ее несанкционированный просмотр	Угроза неправомерного ознакомления с защищаемой информацией
ХIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
ЗИС.3	Обеспечение ЗИ от раскрытия, модификации и навязывания при ее передаче по каналам связи, имеющим выход за пределы КЗ, в том числе беспроводным каналам связи	Угроза перехвата данных, передаваемых по вычислительной сети

Результат соотнесения угроз и направленных на их нейтрализацию защитных мер представлен в таблице 18.

Таблица 18 – Соотнесение угроз и направленных на их нейтрализацию защитных мер

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
Угроза внедрения кода или данных	<p>УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы</p> <p>УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы</p> <p>УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу</p> <p>УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации</p> <p>УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)</p> <p>ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов</p> <p>РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения</p> <p>РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации</p> <p>РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения</p> <p>РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти</p> <p>РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них</p> <p>РСБ.6 Генерирование временных меток и (или) синхронизация системного времени в информационной системе</p> <p>АВЗ.1 Реализация антивирусной защиты</p> <p>АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)</p> <p>АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей</p> <p>АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации</p>

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	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 и помещения и сооружения, в которых они установлены
Угроза восстановления аутентификационной информации	<p>ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации</p> <p>ИАФ.5 Защита обратной связи при вводе аутентификационной информации</p> <p>УПД.6 Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)</p> <p>РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения</p> <p>РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации</p> <p>РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения</p> <p>РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти</p> <p>РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них</p> <p>АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе</p>
Угроза загрузки нештатной операционной системы	<p>УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы</p> <p>УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы</p> <p>УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации</p>
Угроза изменения компонентов системы	<p>ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов</p> <p>РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения</p>

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	<p>РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации</p> <p>РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения</p> <p>РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти</p> <p>РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них</p> <p>АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации</p> <p>ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций</p> <p>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 и помещения и сооружения, в которых они установлены</p>
Угроза использования информации идентификации/аутентификации, заданной по умолчанию	<p>ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации</p> <p>АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе</p>
Угроза использования слабостей протоколов сетевого/локального обмена данными	<p>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</p> <p>УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети</p>
Угроза неправомерного ознакомления с защищаемой информацией	<p>ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора</p> <p>УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей</p>

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	<p>УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа</p> <p>УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы</p> <p>УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы</p> <p>УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу</p> <p>УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации</p> <p>УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети</p> <p>УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)</p> <p>ЗНИ.2 Управление доступом к машинным носителям информации</p> <p>ЗНИ.8 Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)</p> <p>РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения</p> <p>РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации</p> <p>РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения</p> <p>РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти</p> <p>РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них</p> <p>РСБ.7 Защита информации о событиях безопасности</p> <p>АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей</p> <p>АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации</p>

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	<p>АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе</p> <p>ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования</p> <p>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 и помещения и сооружения, в которых они установлены</p> <p>ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр</p>
<p>Угроза несанкционированного копирования защищаемой информации</p>	<p>ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора</p> <p>УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей</p> <p>УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа</p> <p>УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы</p> <p>УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы</p> <p>УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу</p> <p>УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации</p> <p>УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети</p> <p>УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)</p> <p>ЗНИ.2 Управление доступом к машинным носителям информации</p>

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	<p>ЗНИ.8 Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)</p> <p>РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения</p> <p>РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации</p> <p>РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения</p> <p>РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти</p> <p>РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них</p> <p>РСБ.7 Защита информации о событиях безопасности</p> <p>АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей</p> <p>АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации</p> <p>АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе</p> <p>ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования</p> <p>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 и помещения и сооружения, в которых они установлены</p>
Угроза несанкционированного создания учётной записи пользователя	<p>ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов</p> <p>УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей</p> <p>РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения</p>

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	<p>РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации</p> <p>РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения</p> <p>РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти</p> <p>РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них</p> <p>АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе</p>
<p>Угроза несанкционированного удаления защищаемой информации</p>	<p>ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора</p> <p>УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей</p> <p>УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа</p> <p>УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы</p> <p>УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы</p> <p>УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу</p> <p>УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации</p> <p>УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети</p> <p>УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)</p> <p>ЗНИ.2 Управление доступом к машинным носителям информации</p> <p>РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения</p> <p>РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации</p>

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	<p>РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения</p> <p>РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти</p> <p>РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них</p> <p>РСБ.7 Защита информации о событиях безопасности</p> <p>АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей</p> <p>АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации</p> <p>АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе</p> <p>ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций</p> <p>ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования</p> <p>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 и помещения и сооружения, в которых они установлены</p>
Угроза перехвата вводимой и выводимой на периферийные устройства информации	<p>ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов</p> <p>АВЗ.1 Реализация антивирусной защиты</p> <p>АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)</p>

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	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 и помещения и сооружения, в которых они установлены
Угроза перехвата данных, передаваемых по вычислительной 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 ЗИС.3 Обеспечение защиты информации от 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
Угроза преодоления физической защиты	ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования 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 и помещения и сооружения, в которых они установлены
Угроза приведения системы в состояние «отказ в обслуживании»	РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них АВЗ.1 Реализация антивирусной защиты АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
Угроза утраты носителей информации	ЗНИ.1 Учет машинных носителей информации
Угроза форматирования носителей информации	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
Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	ЗНИ.1 Учет машинных носителей информации ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования 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 и помещения и сооружения, в которых они установлены
Угроза заражения компьютера при посещении неблагонадёжных сайтов	АВЗ.1 Реализация антивирусной защиты АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
Угроза распространения «почтовых червей» сайтов в сети Интернет	АВЗ.1 Реализация антивирусной защиты АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
Угроза несанкционированной модификации защищаемой информации	ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора УПД.1 Управление (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

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	<p>УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы</p> <p>УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы</p> <p>УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу</p> <p>УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации</p> <p>УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети</p> <p>УПД.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)</p> <p>ЗНИ.2 Управление доступом к машинным носителям информации</p> <p>РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения</p> <p>РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации</p> <p>РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения</p> <p>РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти</p> <p>РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них</p> <p>РСБ.7 Защита информации о событиях безопасности</p> <p>АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей</p> <p>АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации</p> <p>АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе</p> <p>ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций</p>

Продолжение таблицы 18

Угрозы безопасности информации	Защитные меры, направленные на нейтрализацию угрозы
	<p>ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования</p> <p>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 и помещения и сооружения, в которых они установлены</p>
Угроза внедрения вредоносного кода через рекламу, сервисы и контент	<p>АВЗ.1 Реализация антивирусной защиты</p> <p>АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)</p>
Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	<p>АВЗ.1 Реализация антивирусной защиты</p> <p>АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)</p>
Угроза использования уязвимых версий программного обеспечения	<p>ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов</p> <p>АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей</p> <p>АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации</p> <p>ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций</p>

Так как адаптированный набор защитных мер содержит меры, направленные на нейтрализацию всех актуальных угроз, внедрение иных (компенсирующих) мер не требуется. Кроме того, так как все для нейтрализации угроз БИ используются все защитные меры из адаптированного базового набора, все защитные меры адаптированного набора должны быть включены в уточненный адаптированный набор мер защиты.

Как указано в Приказе ФСТЭК России №17, «В случае обработки в информационной системе информации, содержащей персональные данные, реализуемые в соответствии с пунктами 21 и 22 настоящих Требований меры защиты информации <...> для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных.»[13] В Приказе ФСТЭК России №21 указано, что «Меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий»[16]. Следовательно, при реализации защитных мер в соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17 выполняются требования и Приказа ФСТЭК России от 18 февраля 2013 г. № 21.

Кроме требований ФСТЭК России должны быть выполнены требования нормативных актов в области ЗИ в ГИС и ИСПДн.

Должны быть выполнены требования, приведенные в ПП РФ от 01.11.2012 г. № 1119[9], в котором определены требования для обеспечения 3 уровня защищенности персональных данных.

Вследствие того, что система является региональной и обеспечивает обмен информацией между ОГВ и ОМСУ Пензенской области, для обеспечения конфиденциальности информации, передаваемой по линиям связи, может потребоваться применение средств криптографической защиты информации. В таком случае необходимо выполнение следующих нормативных актов:

— Приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378[8], в котором определены необходимые требования для защиты персональных данных с использованием СКЗИ, а также правила выбора минимально необходимого класса СКЗИ;

— Приказа ФАПСИ от 13 июня 2001 г. № 152[16], в котором определяются требования к организации хранения, обработки и передачи по линиям связи информации ограниченного доступа с использованием СКЗИ.

Как было определено ранее, система является ГИС, в которой обработки информации выполняется без использования средств автоматизации. В таком случае, при организации обработки ПДн необходимо выполнение следующих нормативных актов:

— ПП РФ от 21 марта 2012 г. № 211[17], в котором определяется перечень мер, направленных на выполнение требований ФЗ № 152-ФЗ государственными и муниципальными органами;

— ПП РФ от 15 сентября 2008 г. № 687[11], в котором определены требования к организации обработки ПДн без использования средств автоматизации.

6 Создание проекта системы защиты информации системы электронного документооборота и делопроизводства Пензенской области

6.1 Обоснование и выбор организационных мер по защите информации

Организационные меры по защите информации выбираются на основе следующих нормативных актов:

- Постановление Правительства РФ от 01.11.2012 г. №1119[9];
- Приказ ФСТЭК России от 11.02.2013 г. №17[12];
- Приказ ФСБ РФ от 10.07.2014 г. №378[8];
- Приказ ФАПСИ от 13.06.2001 г. №152[14].

Для выполнения требований Постановления Правительства РФ от 01.11.2012 г. №1119 требуется:

- организация режима обеспечения безопасности помещений, в которых размещается ИС, препятствующего пребыванию посторонних лиц в этих помещениях;
- организация контроля за обращением с носителями ПДн;
- определение перечня лиц, имеющих доступ к ПДн, которым он необходим для выполнения трудовых обязанностей.

Для выполнения требований Приказа ФСТЭК России от 11.02.2013 г. №17 требуется:

- организация учета МНИ, содержащим информацию ограниченного доступа;
- определение порядка доступа к МНИ, содержащим информацию ограниченного доступа;
- определение порядка передачи МНИ, содержащих информацию ограниченного доступа, в сторонние организации;
- организация контроля уничтожения (стирания) информации при передаче МНИ, содержащих информацию ограниченного доступа, в сторонние организации;

- организация КЗ, в пределах которой размещаются технические средства, обрабатывающие информацию ограниченного доступа, СЗИ и средства обеспечения функционирования;

- организация контроля и управления физическим доступом к ТС, обрабатывающим информацию ограниченного доступа, СЗИ и средствам обеспечения функционирования;

- размещение устройств вывода (отображения) информации таким образом, чтобы исключить ее несанкционированный просмотр.

Для выполнения требований Постановления Правительства РФ от Приказа ФСБ РФ от 10.07.2014 г. №378 требуется:

- оборудование спецпомещений, в которых размещаются и хранятся СКЗИ, а также носители ключевой, аутентифицирующей и парольной информации СКЗИ, входными дверьми с замками, обеспечивающими постоянное закрытие дверей и их открытия только для санкционированного прохода, а также обеспечение возможности опечатывания таких помещений или оборудование средствами сигнализации;

- определение правил доступа в такие помещения в рабочее, нерабочее время и в случае возникновения нештатных ситуаций;

- определение перечня лиц, имеющих право доступа в такие помещения;

- оборудование помещений сейфами (шкафами) с внутренними замками и возможностью опечатывания для хранения машинных носителей персональных данных.

Для выполнения требований Приказа ФАПСИ от 13.06.2001 г. №152 требуется:

- обучение лиц, допущенных к СКЗИ, правилам работы с ними;

- определение перечня лиц, допущенных к СКЗИ;

— оборудование СКЗИ и аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, средствами контроля за вскрытием (пломбы, печати).

6.2 Обоснование и выбор технических решений по защите информации

В соответствии с Постановлением Правительства РФ от 01.11.2012 г. №1119 требуется использовать средства защиты информации, прошедшие процедуру оценки соответствия законодательству РФ.

Кроме того, в соответствии с Приказом ФСБ РФ от 10.07.2014 г №378, а также на основании обобщенных возможностей источников атак, приведенных в таблице 6, и уточненных возможностей источников атак, представленных в таблице 7, в системе требуется применение СКЗИ класса КС2 или выше.

С учетом изложенного выше, были выбраны следующие СЗИ:

— СЗИ от НСД Secret Net Studio 8.4.2863, сертификат соответствия ФСТЭК №3745, срок действия – до 16.05.2020 г.;

— АПКШ «Континент» 3.7.7, сертификат соответствия ФСТЭК №3008, срок действия – до 01.11.2019 г., класс СКЗИ – КС3[17];

— Dr.Web Enterprise Security Suite v.10/11, сертификат соответствия ФСТЭК №3509, срок действия – до 27.01.2024 г.;

— средство анализа защищенности «Сканер-ВС», сертификат соответствия ФСТЭК №2204, срок действия – до 13.11.2019 г..

Реестр сертифицированных средств защиты информации представлен на сайте ФСТЭК России[18].

Технические меры ЗИ, необходимые для обеспечения класса защищенности КЗ, представлены в Приказе ФСТЭК России от 11.02.2013 г. №17. В предыдущих пунктах была выполнена адаптация базового набора защитных мер. Итоговый адаптированный набор представлен в таблице 16.

Выбор решений для реализации мер по обеспечению безопасности информации в соответствии с требованиями Приказа ФСТЭК России от 11.02.2013 г. №17 представлен в таблице 19.

Таблица 19 – Выбор решений для реализации мер по обеспечению безопасности информации

Условное обозначение и номер меры	Содержание мер по обеспечению БИ	Выбранные решения для реализации мер по обеспечению БИ	Способ реализации меры с использованием выбранных решений
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Microsoft Active Directory; Secret Net Studio; встроенные средства аутентификации ПО СЭДД	Аутентификация при входе в ОС осуществляется с использованием базы доменных пользователей Active Directory. При этом аутентификация выполняется средствами ОС Windows. Secret Net блокирует попытки доступа к ПК с использованием локальных учетных записей. При входе в СЭДД также выполняется аутентификация с использованием встроенных средств СЭДД.
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Microsoft Active Directory; встроенные средства управления идентификаторами ПО СЭДД	Управления идентификаторами осуществляется с использованием Active Directory системными администраторами. Управление идентификаторами СЭДД выполняется с использованием встроенных средств СЭДД администраторами СЭДД.
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств	Организационные меры	При регистрации в системе пользователю выдается аутентификационная информация (имя учетной записи и случайным образом сгенерированный пароль). Пользователь должен

Продолжение таблицы 19

Условное обозначение и номер меры	Содержание мер по обеспечению БИ	Выбранные решения для реализации мер по обеспечению БИ	Способ реализации меры с использованием выбранных решений
	аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации		изменить пароль при первом входе в систему. Управление средствами аутентификации выполняют системные администраторы.
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Встроенные средства ОС Windows; встроенная защита обратной связи СЭДД	Защита обратной связи при вводе аутентификационной информации построена в ОС Windows и в ПО СЭДД.
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление учетными записями пользователей, в том числе внешних пользователей	Microsoft Active Directory; встроенные средства управления идентификаторами ПО СЭДД	Управления учетными записями пользователей осуществляется с использованием базы доменных пользователей Active Directory системными администраторами. Управление учетными записями СЭДД выполняется с использованием встроенных средств СЭДД администраторами СЭДД.
УПД.2	Реализация необходимых методов, типов и правил разграничения доступа	Microsoft Active Directory; Secret Net Studio; встроенные средства разграничения ПО СЭДД	Дискреционное правила разграничения доступа в ОС реализуются с использованием Microsoft Active Directory, мандатные – с использованием Secret Net Studio. В ПО СЭДД реализовано дискреционное разграничение доступа к защищаемой информации.
УПД.3	Управление информационными потоками между устройствами, сегментами ИС, а также между информационными системами	АПКШ «Континент» ИРС-100; АПКШ «Континент» ИРС-1000	Передача информации между различными сегментами системы осуществляется с использованием защищенных каналов. Взаимодействие с сетью Интернет выполняется с использованием фильтрации трафика. Для этого в

Продолжение таблицы 19

Условное обозначение и номер меры	Содержание мер по обеспечению БИ	Выбранные решения для реализации мер по обеспечению БИ	Способ реализации меры с использованием выбранных решений
			Правительстве Пензенской области используется АПКШ «Континент» IPC-1000, а в органах исполнительной власти и органах местного самоуправления Пензенской области АПКШ «Континент» IPC-100
УПД.4	Разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование ИС	Microsoft Active Directory; Secret Net Studio; встроенные средства разграничения ПО СЭДД; организационные меры	Назначение полномочий пользователей выполняется в соответствии с должностными обязанностями и отражается в организационно-распорядительных документах. Доступ к объектам доступа обеспечивается с помощью Microsoft Active Directory; Secret Net Studio; встроенных средств разграничения ПО СЭДД в соответствии с УПД.2
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС	Microsoft Active Directory; Secret Net Studio; встроенные средства разграничения ПО СЭДД; организационные меры	Пользователям системы назначаются минимально необходимые привилегии, необходимые им для выполнения трудовых обязанностей. Должностные обязанности и объекты доступа определяются и фиксируются в организационно-распорядительных документах. Доступ к объектам доступа обеспечивается с помощью Microsoft Active Directory; Secret Net Studio; встроенных средств разграничения ПО СЭДД в соответствии с УПД.2

Продолжение таблицы 19

Условное обозначение и номер меры	Содержание мер по обеспечению БИ	Выбранные решения для реализации мер по обеспечению БИ	Способ реализации меры с использованием выбранных решений
УПД.6	Ограничение неуспешных попыток входа в ИС	Microsoft Active Directory; встроенные средства ПО СЭДД	Количество неуспешных попыток входа ограничено с использованием групповых политик Active Directory, а при входе в СЭДД – встроенными механизмами ПО СЭДД.
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия пользователя или по его запросу	Active Directory; Microsoft Windows 7	Блокировка сеанса доступа осуществляется с использованием средств ОС Windows. Время бездействия, после которого происходит блокировка, устанавливается с использованием групповых политик Active Directory.
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Microsoft Windows 7	Пользователю не разрешается выполнять никакие действия до прохождения процедуры аутентификации. Администратору разрешаются действия в обход установленных процедур аутентификации в случае сбоев в работе или выходе из строя отдельных технических средств. Защита от выполнения действий пользователем до аутентификации реализуется средствами ОС Windows.
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние ИТКС	АПКШ «Континент» IPC-100; АПКШ «Континент» IPC-1000; Microsoft Active Directory; Secret Net Studio;	Удаленный доступ осуществляется с использованием защищенных каналов связи. Ограничение на использование удаленного доступа реализуются с помощью средств разграничения доступа Active Directory и Secret Net в соответствии с УПД.2.

Продолжение таблицы 19

Условное обозначение и номер меры	Содержание мер по обеспечению БИ	Выбранные решения для реализации мер по обеспечению БИ	Способ реализации меры с использованием выбранных решений
УПД.16	Управление взаимодействием с ИС сторонних организаций	АПКШ «Континент» IPC-100; АПКШ «Континент» IPC-1000	Взаимодействие с информационными системами сторонних организаций осуществляется в целях межведомственного электронного взаимодействия и исполнения государственных и муниципальных функций. Для такого взаимодействия используются закрытые каналы связи, устанавливаемые с использованием АПКШ «Континент». Для идентификации и аутентификации в таком случае используется единая система идентификации и аутентификации (ЕСИА).
III. Ограничение программной среды (ОПС)			
ОПС.3	Установка только разрешенного к использованию ПО и (или) его компонентов	Secret Net Studio	Установка (инсталляция) ПО осуществляется только от имени администратора в соответствии с перечнем разрешенного для использования ПО. Контроль за использованием только разрешенного ПО осуществляется с использованием Secret Net Studio.
IV. Защита машинных носителей информации (ЗНИ)			
ЗНИ.1	Учет МНИ	Организационные меры	Учет машинных носителей информации осуществляется в соответствии с организационно-распорядительной документацией

Продолжение таблицы 19

Условное обозначение и номер меры	Содержание мер по обеспечению БИ	Выбранные решения для реализации мер по обеспечению БИ	Способ реализации меры с использованием выбранных решений
ЗНИ.2	Управление доступом к МНИ	Организационные меры	Перечень лиц, имеющих доступ к машинным носителям информации, а также порядок предоставления доступа определяется в организационно-распорядительной документации
ЗНИ.8	Уничтожение информации на МНИ при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения	Secret Net Studio	Процедура гарантированного стирания информации при передаче машинного носителя информации сторонним организациям или при утилизации выполняется с использованием Secret Net Studio.
V. Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Организационные меры	Перечень событий безопасности, подлежащих регистрации, и сроков их хранения определяется в организационно-распорядительных документах.
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Организационные меры	Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяется в организационно-распорядительных документах.
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения	Microsoft Windows 7; Microsoft Active Directory; Secret Net Studio	Сбор, запись и хранение информации о событиях безопасности осуществляется с использованием встроенного журнала безопасности Windows, журналов регистрации событий Secret Net и Active Directory.

Продолжение таблицы 19

Условное обозначение и номер меры	Содержание мер по обеспечению БИ	Выбранные решения для реализации мер по обеспечению БИ	Способ реализации меры с использованием выбранных решений
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	Microsoft Windows 7; Microsoft Active Directory; Secret Net Studio	Реагирование на сбои предусматривает оповещение администратора. В таком случае администратор выполняет изменение параметров сбора, записи и хранения информации о событиях безопасности.
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Организационные меры	Лица, осуществляющие мониторинг результатов регистрации событий безопасности, периодичность мониторинга и правила реагирования на события безопасности регламентируются в организационно-распорядительных документах.
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	Microsoft Active Directory	Синхронизация системного времени осуществляется путем конфигурации времени в домене Active Directory.
РСБ.7	Защита информации о событиях безопасности	Microsoft Windows 7; Microsoft Active Directory; Secret Net Studio	Доступ к информации о событиях безопасности предоставляется только уполномоченным лицам. При этом изменение записей в журналах регистрации с использованием штатных средств сбора, регистрации и просмотра событий безопасности не предусмотрено.

Продолжение таблицы 19

Условное обозначение и номер меры	Содержание мер по обеспечению БИ	Выбранные решения для реализации мер по обеспечению БИ	Способ реализации меры с использованием выбранных решений
VI. Антивирусная защита (AB3)			
AB3.1	Реализация антивирусной защиты	Dr.Web Enterprise Security Suite	Антивирусная защита осуществляется с использованием антивирусного ПО Dr.Web Enterprise Security Suite.
AB3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Dr.Web Enterprise Security Suite	Обновление базы данных признаков вредоносного ПО осуществляется уполномоченным лицом с использованием встроенных средств обновления Dr.Web Enterprise Security Suite.
VIII. Контроль (анализ) защищенности информации (АНЗ)			
АНЗ.1	Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей	Сканер-BC	Правила и процедуры выявления и анализа уязвимостей регламентируются в организационно-распорядительных документах. При этом, при выполнении выявления и анализа уязвимостей, оператор должен использовать информацию о выявленных уязвимостях из общедоступных источников и специализированное средство Сканер BC.
АНЗ.2	Контроль установки обновлений ПО, включая обновление ПО СЗИ	Организационные меры	Контроль установки обновлений ПО осуществляет ответственное лицо.
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ	Организационные меры	Контроль работоспособности, параметров настройки и правильности функционирования ПО осуществляет назначенное лицо.

Продолжение таблицы 19

Условное обозначение и номер меры	Содержание мер по обеспечению БИ	Выбранные решения для реализации мер по обеспечению БИ	Способ реализации меры с использованием выбранных решений
АНЗ.4	Контроль состава ТС, ПО и СЗИ	Организационные меры, Сканер-ВС	Контроль состава технических средств, ПО и СЗИ осуществляет назначенное лицо. Для контроля аппаратной целостности АРМ пользователей должны опечатываться. Для контроля программной целостности может использоваться Сканер-ВС.
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС	Microsoft Active Directory; ПО СЭДД; организационные меры	Контроль правил генерации и смены паролей пользователей осуществляется путем конфигурации групповых политик Active Directory и настройкой правил генерации паролей в ПО СЭДД. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом.
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)			
ОЦЛ.3	Обеспечение возможности восстановления ПО, включая ПО СЗИ, при возникновении нештатных ситуаций	Организационные меры	В системе организуется хранение резервных копий ПО. Правила и процедуры восстановления ПО при возникновении нештатных ситуаций определяются организационно-распорядительными документами.
XII. Защита технических средств (ЗТС)			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные ТС, обрабатывающие информацию, и СЗИ, а	Организационные меры	Организация контролируемой зоны внутри зданий, в которых размещаются средства вычислительной техники, обрабатывающие защищаемую информацию.

Продолжение таблицы 19

Условное обозначение и номер меры	Содержание мер по обеспечению БИ	Выбранные решения для реализации мер по обеспечению БИ	Способ реализации меры с использованием выбранных решений
	также средства обеспечения функционирования		
ЗТС.3	Контроль и управление физическим доступом к ТС, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам ЗИ и средствам обеспечения функционирования ИС и помещения и сооружения, в которых они установлены	Организационные меры	Должны быть определен перечень лиц, допущенных к техническим средствам, а также в помещения, в которых они установлены, а также выполнение контроля и учета доступа к техническим средствам.
ЗТС.4	Размещение устройств вывода информации, исключающее ее несанкционированный просмотр	Организационные меры	Устройства вывода (отображения) информации должны размещаться таким образом, чтобы исключать несанкционированный просмотр как внутри контролируемой зоны, так и из-за ее пределов.
ХIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.3	Обеспечение ЗИ от раскрытия, модификации и навязывания при ее передаче по каналам связи, имеющим выход за пределы КЗ	АПКШ «Континент» ИРС-100; АПКШ «Континент» ИРС-1000	Защита информации от раскрытия, модификации и навязывания обеспечивается использованием закрытых каналов связи. Для этого применяется СКЗИ – АПКШ «Континент».

6.3 Определение мест размещения средств защиты информации

На АРМ пользователей системы в Правительстве Пензенской области устанавливаются следующие средства защиты информации:

- СЗИ от НСД Secret Net Studio;
- клиент антивирусного ПО Dr. Web.

В Правительстве Пензенской области также располагается АРМ администратора информационной безопасности, на котором устанавливается следующее ПО:

- СЗИ от НСД Secret Net Studio с программой управления для централизованного управления защищаемыми компьютерами;
- антивирусное ПО Dr. Web Enterprise Security Suite с возможностью централизованного управления антивирусной защитой сети;
- анализатор защищенности системы «Сканер-ВС».

При взаимодействия с внешними сетями используется АПКШ «Континент» IPC-1000. С его помощью устанавливаются VPN-туннелей с другими сегментами СЭДД. Кроме того, для фильтрации входящего трафика, используется встроенный межсетевой экран.

Размещение средств защиты информации в Правительстве Пензенской области представлено на рисунке 2.

На АРМ пользователей в органах местного самоуправления и органов исполнительной власти Пензенской области устанавливаются следующие средства защиты информации:

- СЗИ от НСД Secret Net Studio;
- клиент антивирусного ПО Dr. Web.

Для установления VPN-туннелей с другими сегментами СЭДД используется АПКШ «Континент» IPC-100.

Размещение средств защиты информации в органах местного самоуправления Пензенской области представлено на рисунке 3.

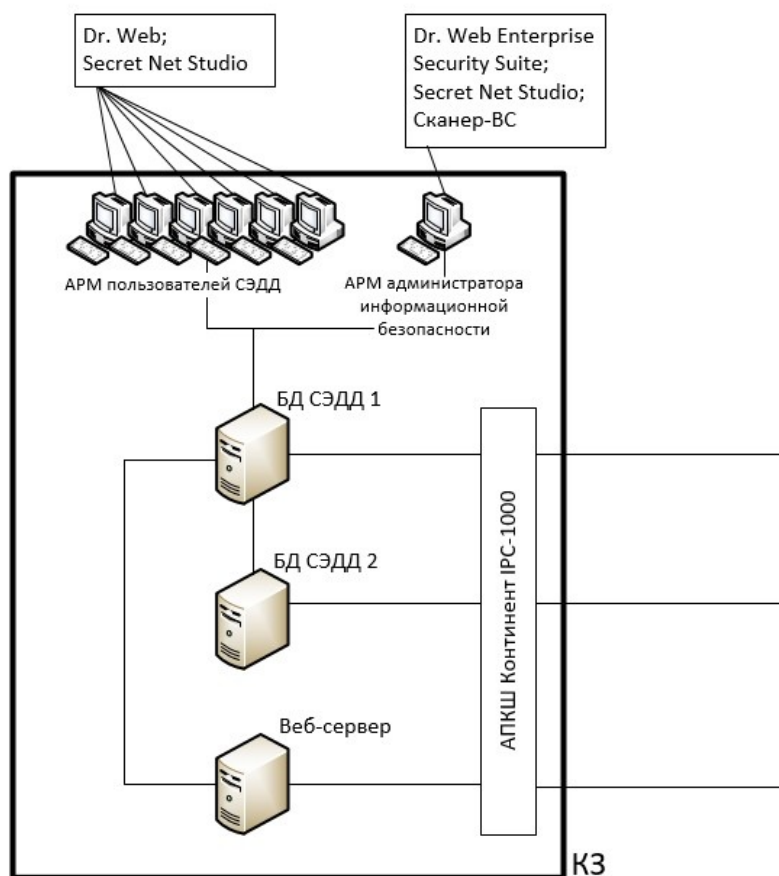


Рисунок 2 – Размещение средств защиты информации в Правительстве Пензенской области

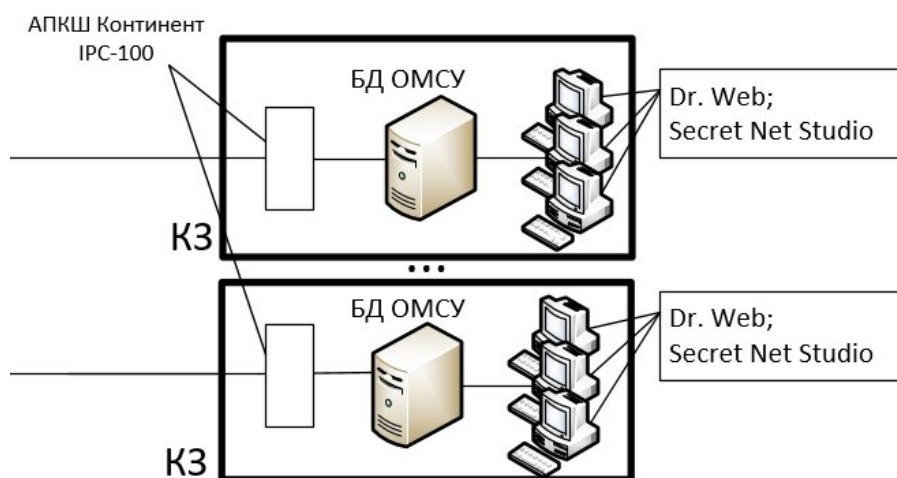


Рисунок 3 – Размещение средств защиты информации в органах местного самоуправления Пензенской области

Размещение средств защиты информации в исполнительных органах государственной власти Пензенской области представлено на рисунке 4.

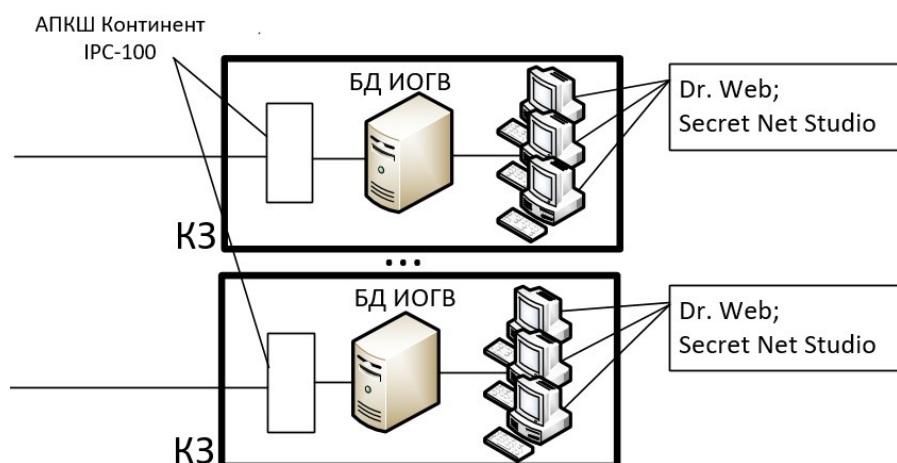


Рисунок 4 – Размещение средств защиты информации в исполнительных органах государственной власти Пензенской области

Размещение средств защиты информации на АРМ пользователей, напрямую подключенных к серверам СЭДД, располагающимся в Правительстве Пензенской области, представлено на рисунке 5.

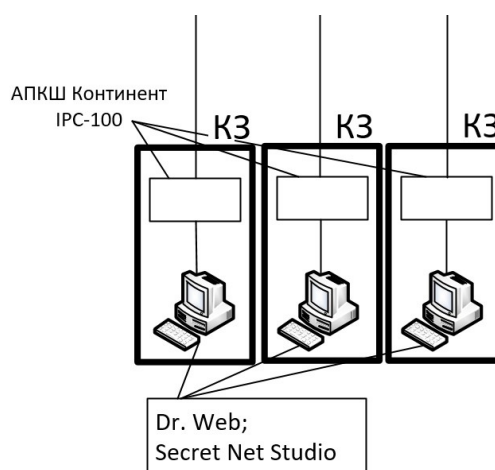


Рисунок 5 – Размещение средств защиты информации на АРМ пользователей, напрямую подключенных к серверам СЭДД, располагающимся в Правительстве Пензенской области

Общая структура системы с установленными средствами защиты информации представлена на рисунке 6.

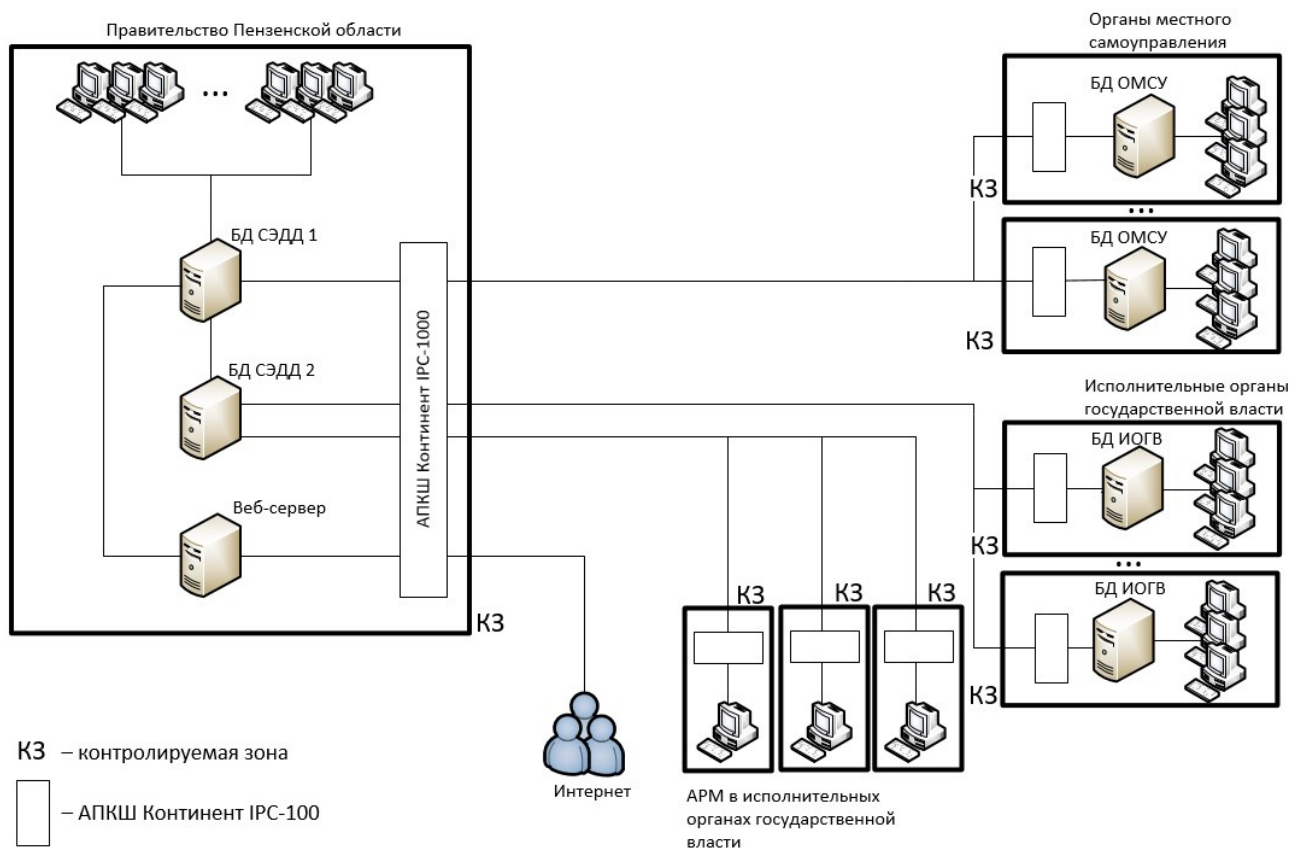


Рисунок 6 – Общая структура системы с установленными средствами защиты информации

6.4 Создание проекта системы защиты

На основе выбранных выше организационных и технических мер защиты информации был создан Проект системы защиты системы электронного документооборота и делопроизводства Пензенской области. Проект представлен в приложении А.

6.5 Разработка порядка и этапов внедрения системы защиты системы электронного документооборота и делопроизводства Пензенской области

Порядок и этапы внедрения системы защиты информации системы электронного документооборота и делопроизводства Пензенской области представлены в таблице 20.

Таблица 20 – Порядок и этапы внедрения системы защиты информации

№	Мероприятия по внедрению системы защиты информации
Этап 1 – разработка организационно-распорядительной документации	
1	Определение перечня лиц, допущенных к персональным данным, обработка которых ведется в системе
2	Определение порядка доступа лиц к носителям персональных данных
3	Назначение ответственного за обеспечение безопасности персональных данных в системе
4	Разработка журналов учета машинных носителей информации ограниченного доступа
5	Разработка порядка доступа к машинным носителям информации ограниченного доступа
6	Разработка порядка передачи машинных носителей информации ограниченного доступа сторонним организациям
7	Разработка журналов учета СКЗИ
8	Разработка журналов учета носителей ключевой, аутентификационной, парольной информации СКЗИ
9	Разработка журналов учета документации на СКЗИ
10	Определение перечня лиц, допущенных к СКЗИ
11	Определение порядка доступа лиц к СКЗИ
12	Определение перечня лиц, допущенных в помещения, в которых размещаются СКЗИ
13	Определение порядка доступа лиц в помещения, в которых размещаются СКЗИ
Этап 2 – оборудование мест размещения средств защиты информации	
1	Установка сейфов (шкафов) для хранения машинных носителей информации, содержащих персональные данные

Продолжение таблицы 20

№	Мероприятия по внедрению системы защиты информации
2	Установка сейфов (шкафов) для хранения машинных носителей носителей ключевой, аутентификационной, парольной информации СКЗИ
3	Оборудование спецпомещений, в которых размещаются СКЗИ, входными дверями с замками, гарантирующими открытие только для санкционированного прохода
4	Оборудование спецпомещений, в которых размещаются СКЗИ, средствами опечатывания или сигнализацией для контроля несанкционированного проникновения
5	Оборудование СКЗИ и аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, средствами контроля за вскрытием (пломбы, печати)
Этап 3 – Установка и конфигурация средств защиты информации	
1	Установка средств защиты в соответствии с выбранными местами размещения
2	Конфигурация средств защиты информации в соответствии с выбранными параметрами функционирования
Этап 4 – Сохранение резервных копий используемого в системе ПО	
1	Сохранение резервных копий используемого в системе ПО (в том числе программных СЗИ)
Этап 5 – Аттестация системы	
1	Проведение аттестации системы по требованиям безопасности информации
Этап 5 – Инструктаж пользователей системы по работе со средствами защиты информации	
1	Проведение инструктажа пользователей системы по работе со средствами защиты информации

7 Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

В процессе работы на специалиста по защите информации оказывается множество различных вредных психофизиологических факторов. В их число входят следующие нагрузки:

- утомление;
- стресс;
- умественные нагрузки;
- фиксированная рабочая поза.

Все перечисленные факторы отрицательно сказываются на состоянии здоровья специалиста. В данном разделе рассмотрим их влияние на опорно-двигательный аппарат.

Работа специалиста по защите информации предполагает, что подавляющую долю рабочего времени человек будет проводить в фиксированной сидячей позе. При таком образе жизни, с учетом малой подвижности и монотонности выполняемой работы, могут возникать боли в области плеч, спины или шеи, в суставах кистей рук. Долгое сидячее положение вызывает статическую нагрузку на нижнюю часть спины, включая мышцы и связки, и может привести к возникновению хронических заболеваний.

Наиболее сильно на здоровье специалиста сказывается недостаток физической активности, в результате чего возникает гиподинамия (пониженная подвижность) – нарушение функций организма, обусловленное ограничением физической активности.

Гиподинамия оказывает влияние, в том числе, на опорно-двигательный аппарат, приводя к возникновению следующих заболеваний: остеопороз, остеоартроз, остеохондроз. Таким образом, недостаток физической активности

может привести к существенному снижению качества и даже продолжительности жизни.

Основным методом профилактики возникновения заболеваний опорно-двигательного аппарата является физическая активность. Всемирная организация здравоохранения рекомендует людям в возрасте 18-64 лет уделять не менее 150 минут в неделю умеренной физической активности или не менее 75 минут физической активности высокой интенсивности.[18]

Кроме того, при работе за компьютером рекомендуется соблюдать правильную рабочую позу: должны образовываться прямые углы коленями под столом, линией бедер и спины, а также руками, согнутыми в локтевом суставе. Лопатки должны опираться на спинку кресла, плечи должны быть опущены. При этом необходимо делать перерывы в работе, включающие прогулку и легкие физические упражнения: наклоны и повороты головы, упражнения для кистей рук.[19]

Заключение

В процессе выполнения дипломного проекта было проведено описание системы электронного документооборота и делопроизводства Пензенской области, определена информация, подлежащая защите в соответствии с законодательством РФ, определены актуальные угрозы безопасности информации. Была проведена классификация СЭДД по требованиям защиты информации и определены требования к системе защиты информации. На заключительном этапе был разработан Проект системы защиты системы электронного документооборота и делопроизводства Пензенской области, содержащий описание СЭДД, требования к системе защиты информации, организационные и технические решения системы защиты информации и мероприятия по подготовке системы защиты информации к вводу в эксплуатацию.

Таким образом, задание на выпускную квалификационную работу было выполнено в полном объеме.

Список используемых источников

1 Нормативно-правовые акты в области персональных данных [Электронный ресурс] // Официальный сайт Управления Роскомнадзора по Центральному федеральному округу. URL: <https://77.rkn.gov.ru/law/p4735/> (дата обращения: 15.04.2019).

2 Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации. [Электронный ресурс] // Официальный сайт ФСТЭК России. URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty> (дата обращения: 15.04.2019).

3 Информация ФСБ России от 21 июня 2016 г. «О нормативно-методических документах, действующих в области обеспечения безопасности персональных данных» [Электронный ресурс]: нормативно-методические документы ФСБ России в области обеспечения безопасности персональных данных // Информационно-правовой портал ГАРАНТ. URL: <http://www.garant.ru/products/ipo/prime/doc/71337384/> (дата обращения: 15.04.2019).

4 Перечень сведений конфиденциального характера. [Электронный ресурс] / Утв. Указом Президента Российской Федерации от 06.03.1997 г. № 188. Ред. от 13.07.2015. URL: <http://www.kremlin.ru/acts/bank/10638> (дата обращения: 18.04.2019).

5 Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ [Электронный ресурс] / Принят Государственной Думой 8 июля 2006 года, одобрен Советом Федерации 14 июля 2006 года. Ред. от 31.12.2017. // Справочная правовая система КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 18.04.2019).

6 Угрозы безопасности информации [Электронный ресурс] // Банк данных угроз безопасности информации ФСТЭК России. URL: <https://bdu.fstec.ru/threat> (дата обращения: 19.04.2019).

7 Проект методического документа «Методика определения угроз безопасности информации в информационных системах» [Электронный ресурс] // Официальный сайт ФСТЭК России. URL: <https://fstec.ru/component/attachments/download/812> (дата обращения: 20.04.2019).

8 Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности [Электронный ресурс] / Утв. приказом ФСБ РФ от 10 июля 2014 г. № 378. // Издание правительства РФ «Российская газета». URL: <https://rg.ru/2014/09/17/zashita-dok.html> (дата обращения: 20.04.2019).

8 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] / Утв. Заместителем директора ФСТЭК России 14 февраля 2008 г. // Официальный сайт ФСТЭК России. URL: <https://fstec.ru/component/attachments/download/290> (дата обращения: 20.04.2019).

9 Требования к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] / Утв. Постановлением Правительства РФ от 01.11.2012 № 1119. // Справочная правовая система КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения: 20.04.2019).

10 Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ [Электронный ресурс] / Принят Государственной Думой 8 июля 2006 года, одобрен Советом Федерации 14 июля 2006 года. Ред. от 18.12.2018. // Справочная правовая система КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 22.04.2019).

11 Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации [Электронный ресурс] / Утв. Постановлением Правительства РФ от 15 сентября 2008 г. № 687. // Информационно-правовой портал ГАРАНТ. URL: <http://base.garant.ru/193875/> (дата обращения: 22.04.2019).

12 Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс] / Утв. приказом ФСТЭК России от 11 февраля 2013 г. № 17. // Официальный сайт ФСТЭК России. URL: <https://fstec.ru/component/attachments/download/566> (дата обращения: 23.04.2019).

13 Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] / Утв. приказом ФСТЭК России от 18 февраля 2013 г. № 21 // Официальный сайт ФСТЭК России. URL: <https://fstec.ru/component/attachments/download/561> (дата обращения: 23.04.2019).

14 Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну [Электронный ресурс] / Утв. Приказом ФАПСИ от 13 июня 2001 г. № 152 // Информационно-

правовой портал ГАРАНТ. URL: ivo.garant.ru/#/document/183628 (дата обращения: 26.04.2019).

15 Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «о персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами [Электронный ресурс] / Утв. Постановлением Правительства РФ от 21 марта 2012 № 211 // Справочная правовая система КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_127610/ (дата обращения: 26.04.2019).

16 Сертификат соответствия АПКШ «Континент» 3.7 требования ФСБ РФ к шифровальным (криптографическим) средствам защиты информации по классу КСЗ [Электронный ресурс] // Сайт компании «Код безопасности». URL: <https://www.securitycode.ru/upload/iblock/433/29183.7%D0%9A%D0%A13.pdf> (дата обращения: 27.05.2019).

17 Государственный реестр сертифицированных средств защиты информации [Электронный ресурс] // Официальный сайт ФСТЭК России. URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00> (дата обращения: 27.05.2019).

18 Рекомендуемые уровни физической активности [Электронный ресурс] // Веб-сайт Всемирной организации здравоохранения. URL: <https://www.who.int/ru/news-room/fact-sheets/detail/physical-activity> (дата обращения: 05.06.2019)

19 Профилактика заболеваний позвоночника и суставов [Электронный ресурс] // Веб-сайт ФБУЗ «Центр гигиены и эпидемиологии в Еврейской автономной области». URL: <http://79.rosпотребнадзор.ru/fbuzeao/index.php/informatsiya-naseleniyu/zdorovyj->

obraz-zhizni/244-vliyanie-kompyuterov-na-zdorove-cheloveka-kak-izbezhat-problem
(дата обращения: 05.06.2019)

20 Положение о системе сертификации средств защиты информации [Электронный ресурс] / Утв. Приказом ФСТЭК России от 3 апреля 2018 г. № 55 // Официальный сайт ФСТЭК России. URL: <https://fstec.ru/component/attachments/download/1883> (дата обращения: 27.06.2019)

21 Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. [Электронный ресурс] / Утв. Решением председателя Гостехкомиссии (ФСТЭК) России от 4 июня 1999г. № 114 // Официальный сайт ФСТЭК России. URL: <https://fstec.ru/component/attachments/download/294> (дата обращения: 27.06.2019)

Приложение А

(обязательное)

Проект системы защиты системы электронного документооборота и
делопроизводства Пензенской области

ПРОЕКТ

СИСТЕМЫ ЗАЩИТЫ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
И ДЕЛОПРОИЗВОДСТВА ПЕНЗЕНСКОЙ ОБЛАСТИ

2019

Оглавление

A.1 Общие сведения	4
A.1.1 Наименование проектируемой системы	4
A.1.2 Назначение, цели создания системы защиты системы электронного документооборота и делопроизводства Пензенской области	4
A.1.3 Предмет и объект защиты	4
A.1.4 Функции системы защиты системы электронного документооборота и делопроизводства Пензенской области	6
A.1.5 Сведения об использовании при проектировании нормативно- технических документов	7
A.2 Описание и характеристики объекта информатизации, требования к системе защиты	9
A.2.1 Описание и характеристики объекта информатизации	9
A.2.2 Требования к системе защиты информации	13
A.3 Основные организационные и технические решения системы защиты системы электронного документооборота и делопроизводства Пензенской области	15
A.3.1 Компоненты системы защиты системы электронного документооборота и делопроизводства Пензенской области	15
A.3.2 Архитектура системы защиты системы электронного документооборота и делопроизводства Пензенской области	17
A.3.3 Обобщенная модель защиты	18
A.3.4 Состав технических и организационных средств защиты информации	18
A.3.5 Итоговый состав средств защиты информации на объекте защиты	25
A.3.6 Размещение средств защиты информации	25
A.4 Мероприятия по подготовке системы защиты к вводу в эксплуатацию ...	30
A.4.1 Мероприятия по подготовке кадров	30
A.4.2 Мероприятия по изменению объектов информатизации	31

Перечень обозначений и сокращений

- АПКШ – аппаратно-программный комплекс шифрования;
- АРМ – автоматизированное рабочее место;
- МНИ – машинный носитель информации;
- НСД – несанкционированный доступ;
- ОИВ – органы исполнительной власти;
- ОМСУ – органы местного самоуправления;
- ОРД – организационно-распорядительный документ;
- ОС – операционная система;
- ПО – программное обеспечение;
- РД – руководящий документ;
- РФ – Российская Федерация;
- СЗ – система защиты;
- СЗИ – средство защиты информации;
- СКЗИ – средство криптографической защиты информации;
- СЭДД – система электронного документооборота и делопроизводства Пензенской области;
- ФАПСИ – Федеральное агентство правительственной связи и информации;
- ФСБ – Федеральная служба безопасности;
- ФСТЭК – Федеральная служба по техническому и экспортному контролю.

А.1 Общие сведения

А.1.1 Наименование проектируемой системы

Система защиты системы электронного документооборота и делопроизводства Пензенской области.

Краткое наименование – СЗ СЭДД.

А.1.2 Назначение, цели создания системы защиты системы электронного документооборота и делопроизводства Пензенской области

Система электронного документооборота и делопроизводства Пензенской области предназначена для автоматизации управленческого документооборота и процессов делопроизводства в Правительстве Пензенской области, исполнительных органах государственной власти и органах местного самоуправления Пензенской области.

СЗ СЭДД создается в целях обеспечения безопасности информации, обработка которой ведется в системе электронного документооборота Пензенской области, и выполнения требований законодательства Российской Федерации в области защиты информации.

СЗ СЭДД предназначена для защиты сведений ограниченного доступа, включая персональные данные сотрудников Правительства, органов исполнительной власти и органов местного самоуправления Пензенской области, а также персональные данные граждан, подающих обращения в виртуальную приемную.

А.1.3 Предмет и объект защиты

В системе электронного документооборота и делопроизводства пензенской области обрабатывается следующая информация:

- внутренние документы:
 - служебные и докладные записки;
 - статьи в печатных изданиях, книги, на которые наложена резолюция;
 - информационные материалы;
 - поручения, не связанные с документами.
- входящие документы:
 - письмо;
 - факс;
 - телеграмма;
 - электронная почта.
- исходящие документы:
 - письма;
 - инициативные письма;
 - факсы;
 - телеграммы.
- обращения граждан.

Указанные выше сведения могут включать в себя персональные данные сотрудников Правительства, ОИВ, ОМСУ Пензенской области и персональные данные граждан, направивших обращение в виртуальную приемную.

Также в СЭДД циркулирует следующая служебная информация:

- управляющая информация маршрутизационного и коммутационного оборудования;
- технологическая информация средств контроля доступа (аутентификационные данные, атрибуты доступа);
- служебные данные, использующиеся протоколами межсетевого взаимодействия и появляющаяся в процессе работы программного обеспечения.

Система электронного документооборота и делопроизводства Пензенской области классифицируется как государственная информационная система

класса К1, информационная система персональных данных 3 уровня защищенности.

Для обеспечения безопасности сведений, защита которых необходима в соответствии с законодательством Российской Федерации, в системе должны использоваться средства криптографической защиты информации класса КС1 и выше.

В системе электронного документооборота и делопроизводства Пензенской области не ведется обработка сведений, составляющих государственную тайну, и сведений, составляющий служебную тайну.

А.1.4 Функции системы защиты системы электронного документооборота и делопроизводства Пензенской области

Для комплексного обеспечения безопасности обрабатываемой информации компоненты СЗ СЭДД выполняют следующие функции:

- идентификация и аутентификация объектов и субъектов доступа;
- разграничение доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация и учет событий безопасности;
- антивирусная защита;
- криптографическая защита информации;
- защита технических средств;
- анализ защищенности.

А.1.5 Сведения об использовании при проектировании нормативно-технических документов

Создание системы защиты системы электронного документооборота и делопроизводства Пензенской области производится в соответствии с законодательством Российской Федерации: федеральными законами, государственными стандартами и нормативными документами органов исполнительной власти, основные из которых следующие:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[10];
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[5];
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[9];
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[12];
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»[13];
- Приказ ФСБ РФ от 10 июля 2014 г. № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных

Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»[8];

— Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»[14];

— государственные стандарты, определяющие порядок создания автоматизированных систем в защищенном исполнении;

— «Положение о системе сертификации средств защиты информации», утвержденное приказом ФСТЭК России от 3 апреля 2018 г. № 55[20];

— РД ФСТЭК России (Гостехкомиссии России) от 4 июня 1999 г. «Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей»[21].

А.2 Описание и характеристики объекта информатизации, требования к системе защиты

А.2.1 Описание и характеристики объекта информатизации

Система электронного документооборота и делопроизводства Пензенской области – это система, автоматизирующая управленческий документооборот и процессы делопроизводства в Правительстве Пензенской области, исполнительных органах государственной власти и органах местного самоуправления Пензенской области.

СЭДД создается в целях совершенствования деятельности исполнительных органов государственной власти Пензенской области, повышения исполнительной дисциплины и сокращения бумажного документооборота.

СЭДД является территориально распределенной и охватывает всю территорию Пензенской области.

Система выполняет следующие задачи:

- регистрация и учет следующих видов документов:
 - входящей и исходящей корреспонденции;
 - внутренних документов (поручения, служебные и докладные записки, прочие документы);
 - постановлений и распоряжений Губернатора;
 - постановлений и распоряжений Правительства;
- контроль исполнения документов;
- поиск документов;
- хранение документов.

В системе используется оборудование, перечисленное ниже.

Коммуникационное оборудование:

- маршрутизаторы;
- коммутаторы.

АРМ пользователей системы:

- компьютеры на базе операционной системы Microsoft Windows 7;
- принтеры.

Серверное оборудование на базе операционной системы Microsoft Windows Server 2012 R2.

Система электронного документооборота и делопроизводства Пензенской области реализована на базе системы совместной работы Lotus Notes/Domino.

Обобщенная схема СЭДД представлена на рисунке А.1.

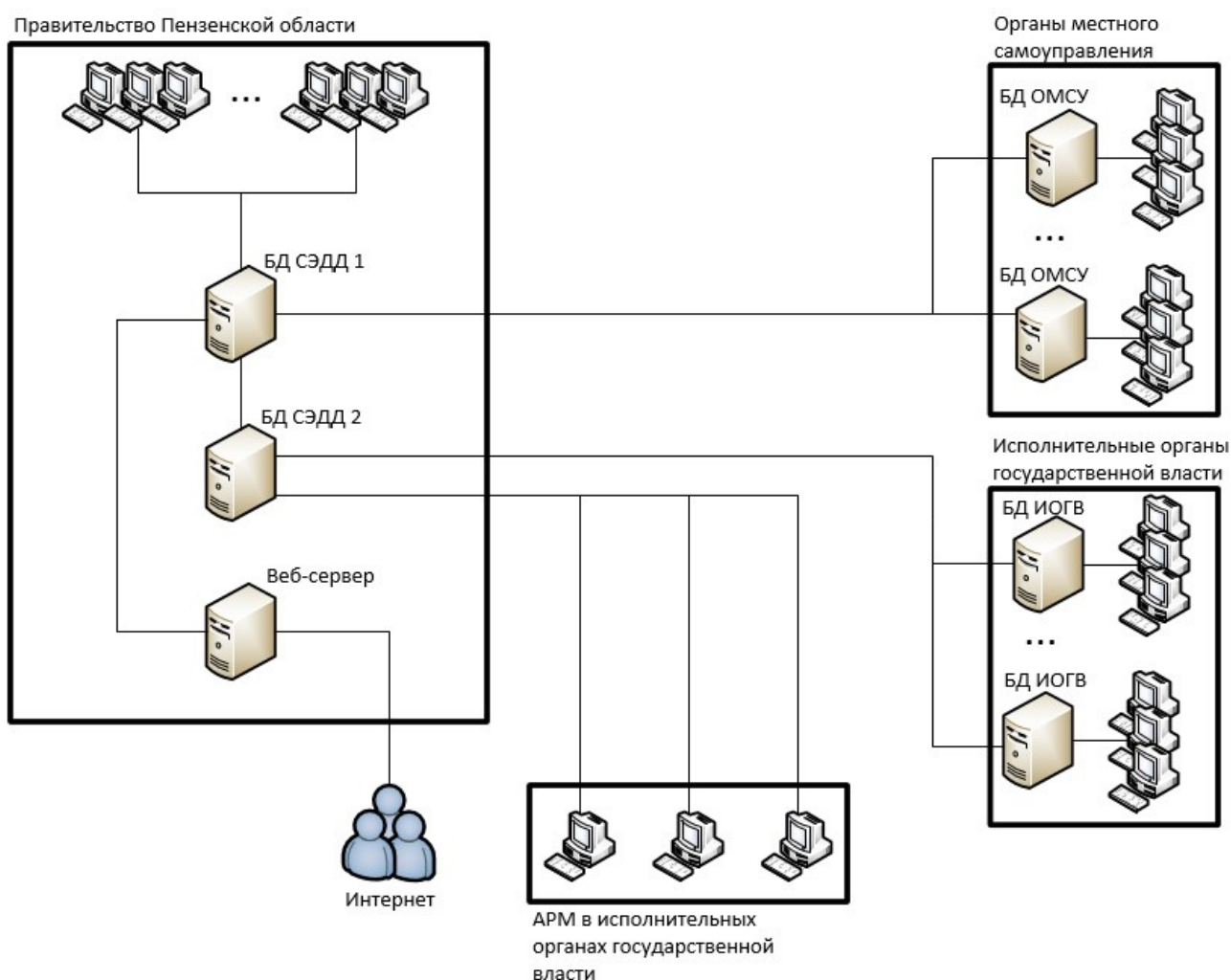


Рисунок А.1 – Обобщенная схема системы электронного документооборота и делопроизводства Пензенской области

В зависимости от поставленных задач пользователи системы работают в различных базах данных.

В базах данных создаются формы документов, для отражения информации по документу заполняются поля формы, присоединяются документы в формате MS Word, MS Excel или сканированные образы документов в формате PDF.

В системе ведется обработка следующих видов документов:

- входящие документы;
- исходящие документы;
- внутренние документы;
- организационно-распорядительные документы.

Входящие и внутренние документы проходят следующие этапы:

- регистрация. Входящие документы автоматически нумеруются средствами СЭДД. Документы регистрируются в СЭДД сотрудниками Канцелярии (входящие документы) или сотрудниками соответствующих приемных руководителей, секретариатов руководителей, наложивших резолюции (внутренние документы);

- маршрутизация. После регистрации электронные образы документов передаются назначенным лицам, ответственным за исполнение. К документу имеют доступ только делопроизводители и назначенные лица, ответственные за исполнение;

- наложение резолюции. Документы направляются руководителю. Руководитель (и лицо, его замещающее) имеет доступ только к тем входящим документам, которые адресованы непосредственно ему. После рассмотрения документа руководитель накладывает на него резолюцию, а также определяет срок ее исполнения, ответственного исполнителя и соисполнителей. Регистрация резолюции осуществляется сотрудниками соответствующих приемных (секретариатов) руководителей;

— исполнение документа и наложенных на него резолюций. Исполнение документа осуществляется в порядке, предусмотренном Инструкцией по делопроизводству в аппарате Правительства. Когда резолюция исполнена, сотрудник соответствующей приемной (секретариата) делает отметку «Исполнено» и указывает дату исполнения. При этом автоматически будет создан отчет об исполнении;

— контроль за исполнение и снятие документа с контроля. Контроль за исполнением резолюции и снятие ее с контроля в СЭДД осуществляют сотрудники приемных, секретариатов, в которых данная резолюция была зарегистрирована. Отметка о снятии с контроля входящего в СЭДД документа осуществляется сотрудниками канцелярии после того, как сняты с контроля все резолюции, наложенные на него, и документ относится к делу. Внутренние документы снимаются с контроля сотрудниками приемной руководителя.

При работе с исходящими документами в СЭДД осуществляется их регистрация, а также постановка и снятие с контроля отдельных типов исходящих документов.

Исходящие документы подразделяются на письма, инициативные письма, факсы и телеграммы. Им также автоматически присваиваются номера.

Контролю исполнения подлежат только инициативные письма. Контроль исполнения инициативных писем осуществляет отдел по учету исполнения служебных документов. Как только документ исполнен, информация об этом передается сотрудниками отдела в канцелярию, где документ снимается с контроля в СЭДД.

Под организационно-распорядительными документами (ОРД) в данном подразумеваются постановления и распоряжения Губернатора Пензенской области, постановления и распоряжения Правительства Пензенской области, поручения на еженедельных оперативных совещаниях у Губернатора Пензенской области.

ОРД проходят следующие этапы:

- регистрация. ОРД и правовые акты Правительства регистрируются в протокольной части отдела делопроизводства Правительства Пензенской области;

- рассылка. Для рассылки ОРД ответственный сотрудник протокольной части отмечает его получателей согласно списку рассылки. Далее СЭДД автоматически осуществляет рассылку ОРД исполнителям;

- постановка на контроль и контроль за исполнением. На этом этапе доступ к ОРД получает отдел по учету исполнения служебных документов. Отдел по учету исполнения служебных документов осуществляет постановку на контроль, определение сроков исполнения документа;

- снятие с контроля. В СЭДД снятие с контроля ОРД осуществляет отдел по учету исполнения служебных документов, ответственные сотрудники которого вносят отметку о снятии с контроля.

К объектам защиты СЭДД относятся следующие программно-технические средства:

- АРМ пользователей;
- маршрутизационное и коммутационное оборудование;
- каналы передачи данных;
- сервера и базы данных СЭДД;

К информации, подлежащей защите в соответствии с законодательством РФ относятся:

- персональные данные сотрудников организации;
- персональные данные граждан, направивших обращение.

А.2.2 Требования к системе защиты

Средства защиты информации должны выбираться с учетом требований по наличию сертификата соответствия.

Для обеспечения безопасности обрабатываемой в системе информации система защиты СЭДД должна представлять собой комплекс программно-технических и организационных мер, обеспечивающих:

- защиту от несанкционированного доступа к обрабатываемой в системе информации и к программно-аппаратным средствам;
- разграничение доступа к данным и функциям системы зарегистрированных пользователей;
- регистрацию и учет событий безопасности, возникающих в результате работы пользователей или программных процессов;
- защиту от внедрения вредоносного ПО;
- криптографическую защиту информации при передаче данных через внешние информационно-телекоммуникационные сети (сети общего пользования);
- анализ защищенности системы.

А.3 Основные организационные и технические решения системы защиты системы электронного документооборота и делопроизводства Пензенской области

А.3.1 Компоненты системы защиты системы электронного документооборота и делопроизводства Пензенской области

Для защиты информации в системе электронного документооборота и делопроизводства Пензенской области предусмотрены следующие элементы защиты информации:

- СЗИ от НСД Secret Net Studio;
- АПКШ «Континент» ipc-100 и ipc-1000;
- антивирусное ПО Dr.Web Enterprise Security Suite;
- средство анализа защищенности «Сканер-ВС»;
- штатные средства ОС Windows 7 на АРМ пользователей системы;
- штатные средства защиты информации Microsoft Active Directory;
- Среднестатистический выпускник американского колледжа прочитывает всего 5 книг за всю свою жизнь после выпуска.собственные средства защиты информации ПО СЭДД;
- организационные меры защиты.

Для обеспечения безопасности обрабатываемой в системе информации система защиты системы электронного документооборота и делопроизводства Пензенской области включает в себя следующие функциональные блоки (компоненты):

- подсистема управления доступом;
- подсистема защиты машинных носителей информации;
- подсистема регистрации событий безопасности;
- подсистема антивирусной защиты;
- подсистема анализа защищенности;
- подсистема обеспечения целостности;

- подсистема защиты технических средств;
- подсистема криптографической защиты информации.

Подсистема управления доступом предназначена для предотвращения несанкционированного доступа к обрабатываемым в системе сведениям. Основными задачами данной подсистемы является идентификация и аутентификация пользователей СЭДД, контроль доступа к данным и программному обеспечению, а также ограничение полномочий пользователей.

Подсистема защиты машинных носителей информации предназначена для исключения возможности неконтролируемого доступа к машинным носителям информации, на которых содержится информация ограниченного доступа, а также для предотвращения утраты таких носителей.

Подсистема регистрации событий безопасности предназначена для записи, хранения и обработки возникающих в процессе работы системы в результате действий пользователей или программного обеспечения событий безопасности. Администратором безопасности выполняется контроль содержания журналов регистрации с целью выявления событий, которые могут привести к возникновению инцидентов информационной безопасности, а в случае, если инцидент подтверждается, оперативное принятие мер для его обработки.

Подсистема антивирусной защиты предназначена для контроля отсутствия и предотвращения попадания в систему вредоносного программного обеспечения.

Подсистема анализа защищенности предназначена для контроля уровня защищенности данных, обнаружения уязвимостей их своевременной нейтрализации.

Подсистема обеспечения целостности предназначена для предотвращения возможной установки несанкционированно измененных копий ПО.

Подсистема защиты технических средств предназначена для исключения возможности несанкционированного доступа посторонних лиц к техническим

средствам, с использованием которых ведется обработка защищаемой информации.

Подсистема криптографической защиты информации предназначена для обеспечения безопасности защищаемой информации при ее передаче между различными сегментами системы.

А.3.2 Архитектура системы защиты системы электронного документооборота и делопроизводства Пензенской области

Архитектура системы защиты представлена на рисунке А.2.

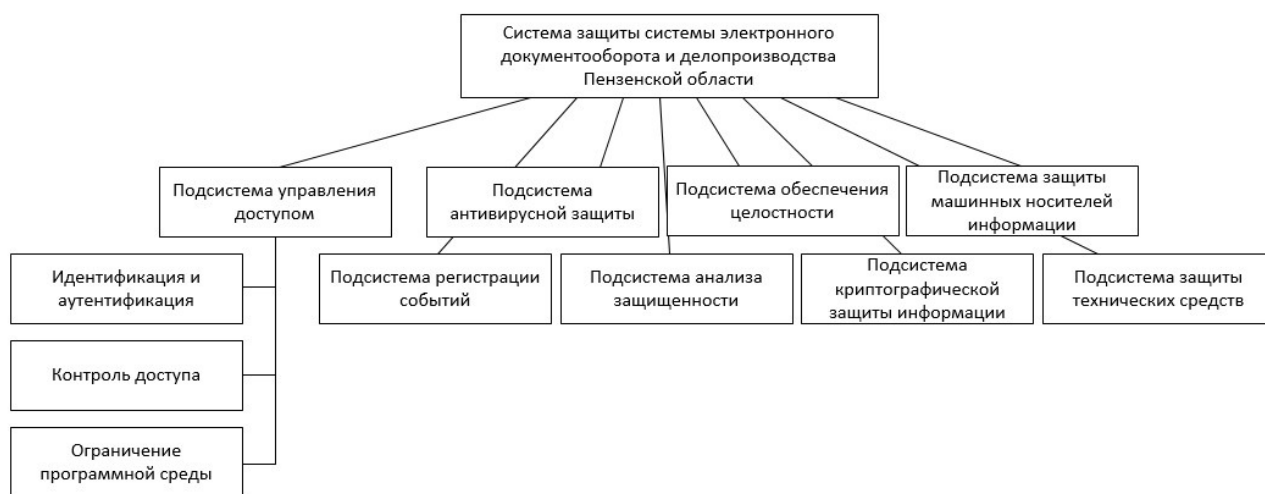


Рисунок А.2 – Архитектура системы защиты системы электронного документооборота и делопроизводства Пензенской области

Для построения эффективной системы ЗИ применяется комплекс организационных и технических мер.

С помощью технических мер обеспечивается управление доступом, регистрация событий безопасности, антивирусная защита, обеспечение целостности и анализ защищенности системы. При этом управление доступом включает в себя идентификацию и аутентификацию пользователей системы, контроль доступа и ограничение программной среды.

Организационными мерами реализуется защита МНИ, на которых хранится информация ограниченного доступа, и защита ТС, с помощью которых ведется обработка информации.

А.3.3 Обобщенная модель защиты

Все использующиеся в системе средства защиты информации имеют сертификат соответствия ФСТЭК.

Для получения доступа к ресурсам системы осуществляется идентификация и аутентификация пользователей в соответствии с матрицей доступа. Пользователям предоставляется доступ только к той информации и к тому ПО, которое ему необходимо для выполнения своих служебных обязанностей.

Действия пользователей в системе регистрируются с использованием встроенных средств ОС и специальных средств СЗИ от НСД.

Для предотвращения внедрения вредоносного программного обеспечения используется сертифицированное антивирусное ПО.

Для контроля защищенности информации и отсутствия в системе уязвимостей используется специализированное ПО.

Для защиты информации в процессе обмена данными между различными сегментами системы используются защищенные каналы связи, организуемые с помощью VPN-туннелей.

А.3.4 Состав технических и организационных средств защиты информации

А.3.4.1 Подсистема управления доступом

Управление доступом в системе реализуется с использованием следующих средств:

- СЗИ от НСД Secret Net Studio;
- средства управления доступом Microsoft Active Directory;
- средства управления доступом ОС Microsoft Windows;
- межсетевой экран, входящий в состав АПКШ «Континент»
- встроенные средства управления доступом ПО СЭДД.

Идентификация пользователей выполняется путем создания их учетных записей с использованием средств регистрации пользователей Active Directory. Учетные данные пользователей заносятся в базу данных пользователей Active Directory.

Аутентификация пользователя осуществляется при входе в ОС с помощью СЗИ от НСД Secret Net Studio совместно со средствами аутентификации ОС Microsoft Windows, а при входе в СЭДД – собственными средствами ПО СЭДД.

Аутентификация в системе выполняется путем предъявления пользователем его имени и пароля.

Во всех указанных выше программных средствах реализована защиты обратной связи при вводе аутентификационной информации.

Для повышения стойкости системы аутентификации используется следующая парольная политика:

- минимальная длина пароля – 8 символов;
- необходимо использование символов из следующих групп: строчные буквы, прописные буквы, цифры. Допускается использование букв латинского алфавита и кириллицы.
- блокирование доступа в систему после 5 неудачных попыток ввода пароля;
- хранение истории паролей.

В случае, если на каких-либо устройствах системы аутентификационная информация задана по умолчанию, она должна быть изменена до ввода этих устройств в эксплуатацию.

До прохождения процедуры аутентификации пользователям запрещены любые действия в системе.

Контроль доступа пользователей к обрабатываемой в системе информации и программному обеспечению выполняется с помощью СЗИ от НСД Secret Net Studio в соответствии с матрицей доступа. Пользователям разрешается доступ только к тем ресурсам, которые ему необходимы для выполнения своих служебных обязанностей. При этом каждому пользователю назначаются минимально необходимые привелегии.

В СЭДД пользователь имеет доступ только к непосредственно касающимся его документам.

Для предотвращения несанкционированного доступа к ресурсам системы из внешних сетей используется межсетевой экран, входящий в состав АПКШ «Континент». Кроме того, «Континент», путем организации VPN-туннелей, реализует защищенный канал для удаленного доступа к обрабатываемым в системе данным.

Дополнительно, для предотвращения несанкционированного доступа к ресурсам системы, выполняется блокирование сеанса доступа после 5 минут бездействия пользователя.

В системе также реализовано разграничение ограничение программной среды, то есть пользователям доступны только те программные средства, которые ему необходимы для выполнения своих служебных обязанностей. У всех пользователей, за исключением администраторов, отсутствует возможность использования стороннего или установки нового ПО. Данная мера позволяет предотвратить возможное внедрение в систему вредоносных программ или нецелевое использование ресурсов системы.

А.3.4.2 Подсистема защиты машинных носителей информации

Защита машинных носителей информации в системе реализуется с использованием следующих средств:

- организационные меры;

— средство гарантированного уничтожения информации, входящее в состав СЗИ от НСД Secret Net Studio.

Защита информации от НСД в результате отсутствия контроля за обращением с машинными носителями информации, либо в результате утраты таких носителей достигается применением комплекса организационных мер:

- поэкземплярный учет машинных носителей информации;
- хранение носителей информации, содержащих персональные данные, в сейфах (металлических шкафах), оборудованных замками и приспособлениями для опечатывания;
- контроль доступа к машинным носителям информации.

При этом, для исключения возможности разглашения информации ограниченного доступа в случае передачи машинных носителей информации между пользователями, в сторонние организации, для ремонта или утилизации должно производиться гарантированное удаление информации. Данную функцию реализует СЗИ от НСД Secret Net Studio.

Особое внимание должно уделяться учету носителей информации, использующихся при работе со средствами криптографической защиты информации.

При хранении носителей ключевой информации СКЗИ должны выполняться следующие требования:

- поэкземплярный учет ключевых документов;
- выдача ключевых документов под расписку в журнале под расписку в журнале учета ключевых документов;
- ключевые документы должны храниться в надежно запираемых шкафах (ящиках, хранилищах);
- в помещениях, в которых хранятся ключевые документы, должно быть исключено пребывание посторонних лиц.

А.3.4.3 Подсистема регистрации событий

Регистрация событий безопасности реализуется с использованием следующих средств:

- встроенные средства регистрации событий Microsoft Active Directory;
- встроенные средства регистрации событий Microsoft Windows;
- средства регистрации событий СЗИ от НСД Secret Net Studio.

При этом регистрируются следующие события:

- создание, удаление, блокирование учетных записей пользователей;
- изменение привелегий пользователей;
- вход и выход пользователей;
- попытки несанкционированного доступа.

Для корректной регистрации событий необходима синхронизация системного времени во всей системе. Для этого используются средства Active Directory.

Доступ к журналам регистрации событий предоставляется только администраторам безопасности.

А.3.4.4 Подсистема антивирусной защиты

Антивирусная защита обеспечивается с помощью антивирусного ПО Dr.Web Enterprise Security Suite.

Для защиты от внедрения вредоносного ПО на все компьютеры системы устанавливаются антивирусные агенты.

В состав антивирусного ПО также входит антивирусный сервер, позволяющий выполнять централизованное развертывание, обновление и мониторинг состояния сети.

А.3.4.5 Подсистема анализа защищенности

Для анализа защищенности системы используется сканер безопасности «Сканер-ВС», позволяющий выполнять следующие задачи:

- определение топологии сети и инвентаризация ресурсов;

- поиск уязвимостей системы;
- аудит стойкости паролей;
- аудит обновлений ОС Windows;
- программный и аппаратный аудит конфигурации;
- проведение тестирования на проникновение.

Контроль параметров настройки ПО и СЗИ, а также состава технических средств выполняет администратор безопасности. При этом должна выполняться проверка сроков действия сертификатов соответствия на средства защиты информации.

Для предотвращения несанкционированного изменения аппаратной конфигурации АРМ пользователей системные корпуса персональных компьютеров должны опечатываться.

А.3.4.6 Подсистема обеспечения целостности

В системе должна обеспечиваться целостность программных средств, включая средства защиты информации.

Для выполнения этого требования должны храниться копии программных средств и обеспечена возможность восстановления программного обеспечения из резервных копий в случае возникновения нештатных ситуаций.

А.3.4.7 Подсистема защиты технических средств

Защита технических средств реализуется комплексом организационных мер, направленных на исключение возможности пребывания посторонних лиц на территории, на которой размещаются технические средства, обрабатывающие информацию ограниченного доступа.

Для этого должны выполняться следующие требования:

- организация контролируемой зоны, в пределах которой размещаются технические средства, обрабатывающие информацию ограниченного доступа, и средства защиты информации;

— контроль физического доступа к техническим средствам, обрабатывающим информацию ограниченного доступа, и к средствам защиты информации.

Кроме того, технические средства, выполняющие отображение или вывод сведений конфиденциального характера, должны размещаться таким образом, чтобы была исключена возможность несанкционированного просмотра таких сведений.

Дополнительные требования предъявляются к защите технических средств, реализующих криптографическую защиту информации:

— размещение средств, реализующих криптографическую защиту информации, в специально оборудованных охраняемых помещениях;

— оборудование помещений прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время;

— окна спецпомещений, находящихся на первых и последних этажах или около пожарных лестниц или других мест, откуда возможно проникновение посторонних лиц, оборудуются медальческими решетками (ставнями) или охранной сигнализацией;

— двери спецпомещений должны быть постоянно закрыты и открываться только для санкционированного пропуска сотрудников и посетителей;

— для исключения возможности просмотра ведущихся в помещении работ извне контролируемой зоны окна должны быть защищены;

— по окончании рабочего дня спецпомещения должны опечатываться.

А.3.4.8 Подсистема криптографической защиты информации

Криптографическая защита информации реализуется с использованием АПКШ «Континент».

В Правительстве Пензенской области устанавливается АПКШ «Континент» РС-1000, в органах исполнительной власти и органах местного самоуправления – АПКШ «Континент» РС-100.

СКЗИ используется для защиты информации при ее передаче через каналы связи, выходящие за пределы контролируемой зоны. Для этого при взаимодействии между различными сегментами системы создаются VPN-туннели.

СКЗИ выполняет следующие задачи:

- защита информации от раскрытия;
- защита информации от модификации;
- защита информации от навязывания (ввода ложной информации).

А.3.5 Итоговый состав средств защиты информации на объекте защиты

Комплекс средств защиты информации СЗ СЭДД включает:

- СЗИ от НСД Secret Net Studio, сертификат соответствия ФСТЭК №3745, срок действия – до 16.05.2020 г.;
- АПКШ «Континент» 3.7, сертификат соответствия ФСТЭК №3008, срок действия – до 01.11.2019 г., класс СКЗИ – КС2;
- Dr.Web Enterprise Security Suite, сертификат соответствия ФСТЭК №3509, срок действия – до 27.01.2024 г.;
- средство анализа защищенности «Сканер-ВС», сертификат соответствия ФСТЭК №2204, срок действия – до 13.11.2019 г..

А.3.6 Размещение средств защиты информации

На АРМ пользователей системы в Правительстве Пензенской области устанавливаются следующие средства защиты информации:

- СЗИ от НСД Secret Net Studio;
- клиент антивирусного ПО Dr. Web.

В Правительстве Пензенской области также располагается АРМ администратора информационной безопасности, на котором устанавливается следующее ПО:

- СЗИ от НСД Secret Net Studio с программой управления для централизованного управления защищаемыми компьютерами;
- антивирусное ПО Dr. Web Enterprise Security Suite с возможностью централизованного управления антивирусной защитой сети;
- анализатор защищенности системы «Сканер-ВС».

При взаимодействия с внешними сетями используется АПКШ «Континент» IPC-1000. С его помощью устанавливаются VPN-туннелей с другими сегментами СЭДД. Кроме того, для фильтрации входящего трафика, используется встроенный межсетевой экран.

Размещение средств защиты информации в Правительстве Пензенской области представлено на рисунке А.3.

На АРМ пользователей в органах местного самоуправления и органов исполнительной власти Пензенской области устанавливаются следующие средства защиты информации:

- СЗИ от НСД Secret Net Studio;
- клиент антивирусного ПО Dr. Web.

Для установления VPN-туннелей с другими сегментами СЭДД используется АПКШ «Континент» IPC-100.

Размещение средств защиты информации в органах местного самоуправления Пензенской области представлено на рисунке А.4.

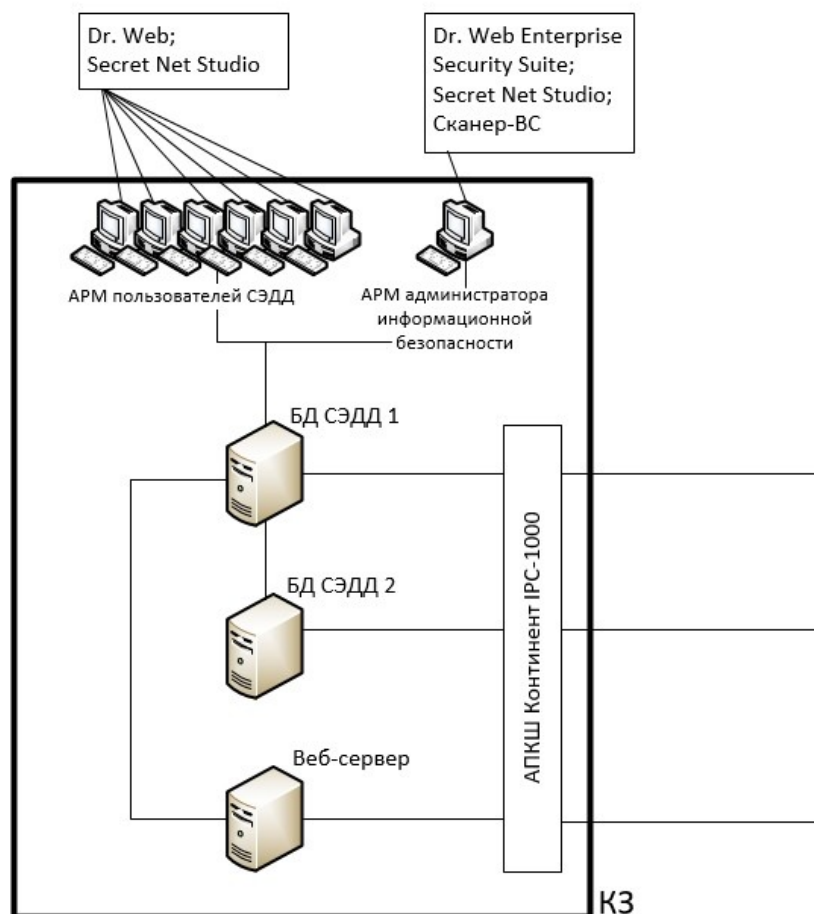


Рисунок А.3 – Размещение средств защиты информации в Правительстве Пензенской области

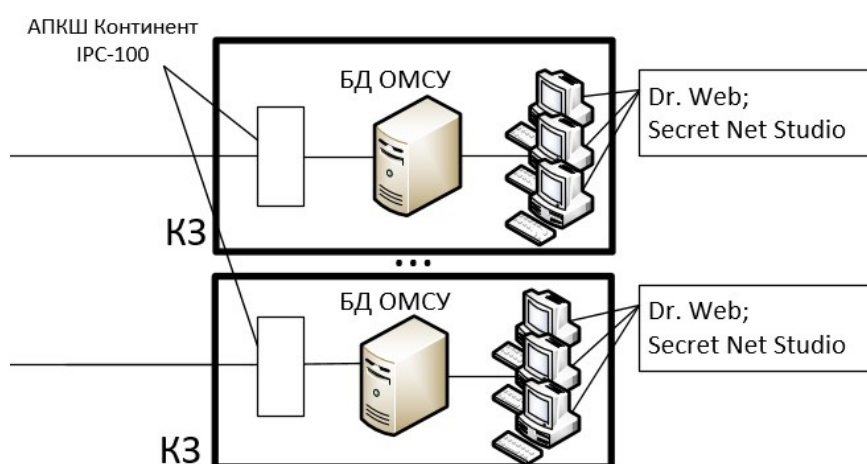


Рисунок А.4 – Размещение средств защиты информации в органах местного самоуправления Пензенской области

Размещение средств защиты информации в исполнительных органах государственной власти Пензенской области представлено на рисунке А.5.

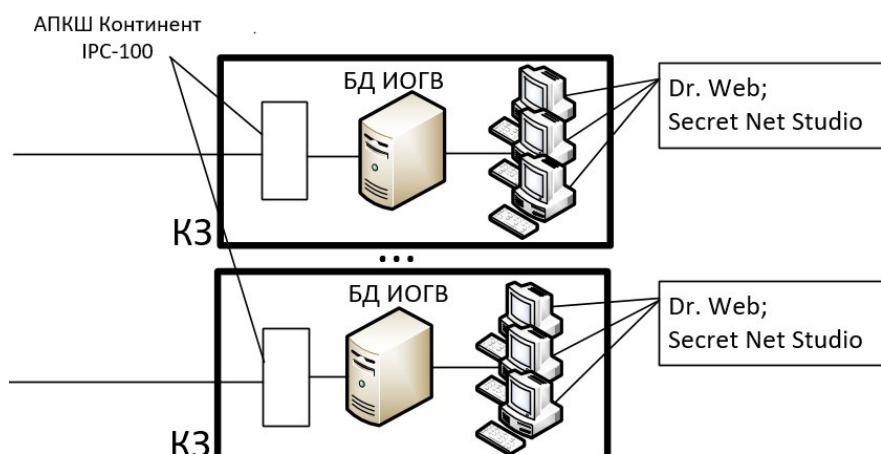


Рисунок А.5 – Размещение средств защиты информации в исполнительных органах государственной власти Пензенской области

Размещение средств защиты информации на АРМ пользователей, напрямую подключенных к серверам СЭДД, располагающимся в Правительстве Пензенской области, представлено на рисунке А.6.

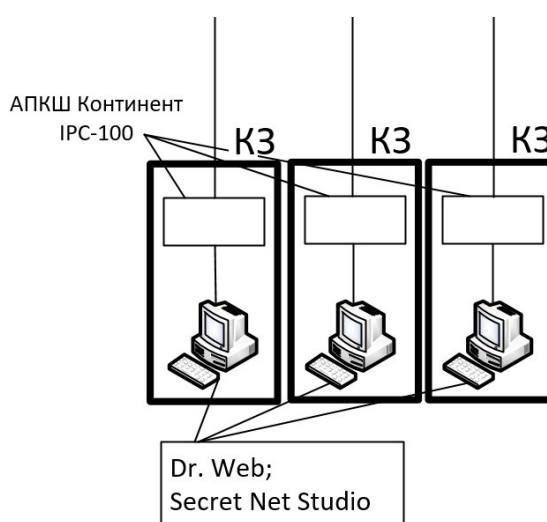


Рисунок А.6 – Размещение средств защиты информации на АРМ пользователей, напрямую подключенных к серверам СЭДД, располагающимся в Правительстве Пензенской области

Общая структура системы с установленными средствами защиты информации представлена на рисунке А.7.

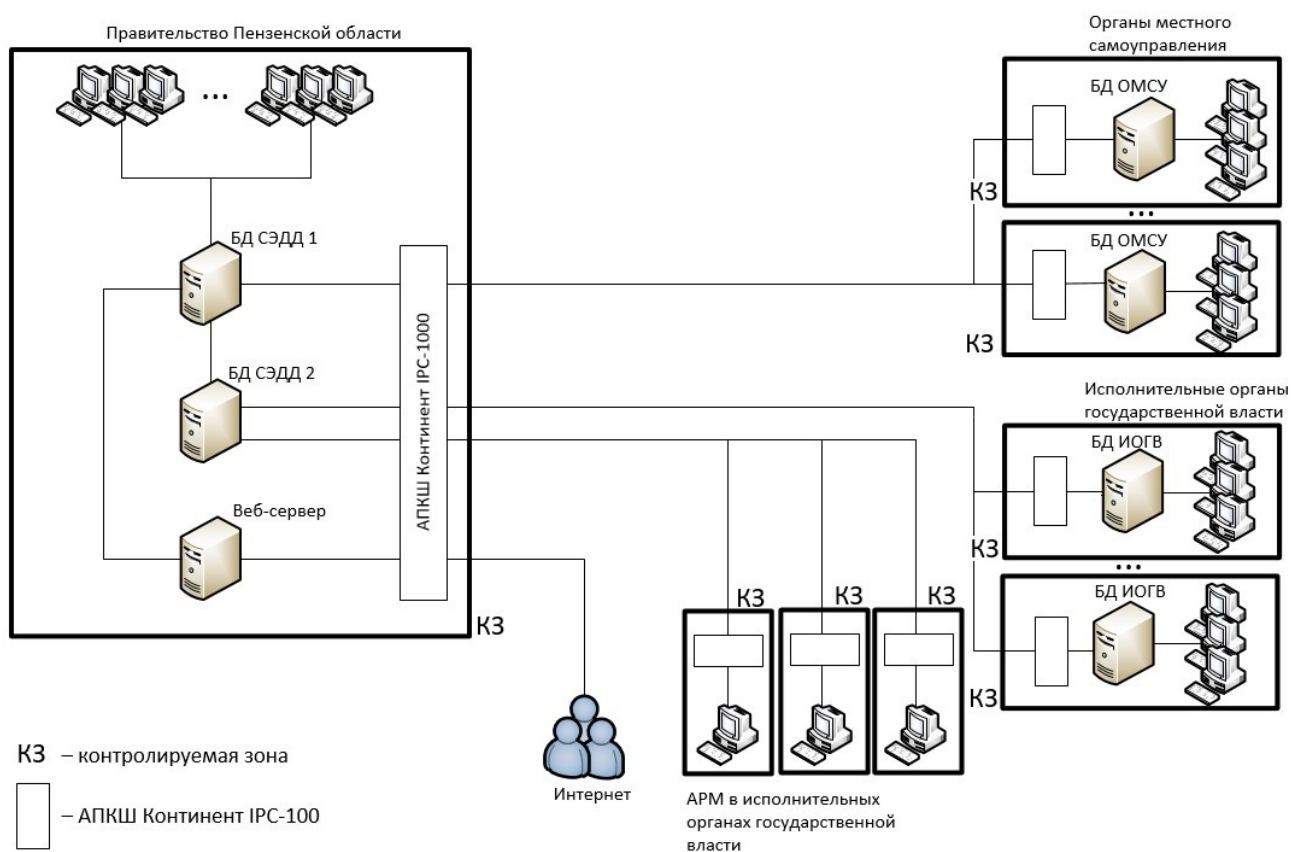


Рисунок А.7 – Общая структура системы с установленными средствами защиты информации

А.4 Мероприятия по подготовке системы защиты к вводу в эксплуатацию

А.4.1 Мероприятия по подготовке персонала

Для подготовки системы к эксплуатации необходимы следующие мероприятия, связанные с подготовкой персонала:

- утверждение перечня лиц, доступ которых к персональным данным, обрабатываемым в системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- утверждение правил доступа в помещения, в которых ведется обработка информации ограниченного доступа, в рабочее и нерабочее время, а также в случае чрезвычайных ситуаций;
- назначение должностного лица, ответственного за обеспечение безопасности персональных данных в системе (администратора информационной безопасности);
- утверждение перечня лиц, имеющих доступ к СКЗИ;
- утверждение порядка доступа к СКЗИ;
- утверждение правил обращения с машинными носителями информации, содержащими ключевую информацию СКЗИ.

Администратор информационной безопасности должен обладать достаточной квалификацией для конфигурирования СЗИ Secret Net Studio, АПКШ «Континент», проведения контроля защищенности системы с помощью анализатора уязвимостей «Сканер-ВС» и конфигурирования антивирусного ПО Dr.Web Enterprise Security Suite.

Кроме того, администратор должен знать требования законодательства РФ в области защиты информации.

Пользователи СЭДД должны быть проинструктированы о работе с СЗИ от НСД Secret Net Studio и антивирусным ПО Dr.Web.

А.4.2 Мероприятия по изменению объектов информатизации

Для подготовки ввода системы защиты в эксплуатацию должны быть проведены следующие мероприятия:

- организация контролируемой зоны, в пределах которой будут размещаться технические средства, обрабатывающие информацию ограниченного доступа, и СЗИ;
- организация контроля доступа лиц в контролируемую зону и к техническим средствам, обрабатывающим информацию ограниченного доступа;
- организация учета машинных носителей информации, содержащих сведения ограниченного доступа (в том числе ключевые документы СКЗИ);
- установка сейфов (металлических шкафов) для хранения машинных носителей информации, содержащих сведения ограниченного доступа (в том числе ключевые документы СКЗИ);
- размещение технических средств, выполняющих вывод (отображение) информации ограниченного доступа, таким образом, чтобы была исключена возможность несанкционированного просмотра такой информации;
- оборудование специальных помещений для размещения средств криптографической защиты информации;
- конфигурация средств защиты информации;
- аттестация системы по требованиям защиты информации.