ВЕСТНИК
ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
МОРСКОГО И РЕЧНОГО ФЛОТА ИМЕНИ АДМИРАЛА С. О. МАКАРОВА

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК-004.056.53

С. С. Соколов,
канд. техн. наук, доцент,
ГУМРФ имени адмирала С. О. Макарова;

С. С. Малов,
старший преподаватель,
ГУМРФ имени адмирала С. О. Макарова;

А. С. Карпина,
студент,
ГУМРФ имени адмирала С. О. Макарова

ПОСТРОЕНИЕ ЗАЩИЩЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ МОНИТОРИНГОВОГО ЦЕНТРА ОКАЗАНИЯ ТЕЛЕМАТИЧЕСКИХ УСЛУГ БЕЗОПАСНОСТИ НА ТРАНСПОРТЕ

CREATION OF THE PERSONAL INFORMATION PROTECTED INFORMATION SYSTEM OF THE RENDERING TELEMATIC SERVICES OF SAFETY ON TRANSPORT MONITORING CENTER

В представленной статье рассматривается процесс построения защищенной информационной системы персональных данных для мониторингового центра оказания телематических услуг безопасности на транспорте. Рассмотрены все основные компоненты обеспечения безопасности: правовой, организационный, программно-технический. Описанное в статье исследование может в широком смысле служить образцом проведения предпроектного обследования объекта информатизации на предмет создания автоматизированной системы в защищенном исполнении.

In the presented article process of creation of the protected information system of personal information for the monitoring center of rendering telematic services of safety on transport is considered. All main components of safety are considered: legislative, organizational, program and technical. The research described in article can serve in a broad sense as a model of carrying out predesign inspection of object of informatization regarding creation of the automated system in the protected execution.

Ключевые слова: информационная безопасность, безопасность мониторингового центра, информационная безопасность на транспорте.

Key words: information security, safety of the monitoring center, information security on transport.

В НАСТОЯЩЕЕ время все большую популярность набирают организации по оказанию удаленных охранных услуг на региональном и федеральном уровнях. В основе их функционирования лежит технология передачи данных (GSM/GPRS) и систем позиционирования (GPS/ГЛОНАСС). Функционал данных мониторинговых центров (далее — МЦ) достаточно широк и включает в себя охранный, противопожарный, технический и информационный мониторинг.

Охрана объектов обеспечивается круглосуточно семь дней в неделю. Пользоваться услугами МЦ финансово выгоднее, чем организовывать полноценную, физическую охрану. А в случае с мобильным объектом (например, автомобилем) — это единственное возможное решение. Клиентское оборудование (датчики движения, перемещения, дыма, объема) своевременно подает сигнал тревоги на диспетчерский пункт централизованного управления, оператор которого вызывает специальные службы реагирования (полицию, скорую помощь, пожарную охрану и др.).

Работа пункта централизованного наблюдения МЦ осуществляется по следующей схеме:

1) с объектового оборудования (модули GSM, контрольные панели, датчики, блоки питания) сигнал поступает на устройство «вычислитель», который определяет примерные координаты объекта;

2) далее сигнал с «вычислителя» поступает на корректирующую матрицу — программу, которая по полученным данным уточняет координаты объекта и рассчитывает местоположение объекта на цифровой карте;

3) диспетчерский пульт централизованного наблюдения и база данных (далее — БД) — аппаратно-программное устройство, которое направляет сигналы и данные по объектам в соответствии с прописанной маршрутизацией на автоматизированные рабочие места (далее — АРМ) и ДПУ и позволяет заполнить информационные поля в АРМ ОД из БД.

Возможности МЦ позволяют к решению любой задачи применять индивидуальный подход. Объектовое оборудование для мониторинга применимо к любой АС. Возможности позволяют осуществить мониторинг технического состояния: бурильного оборудования, нефтедобывающих установок, насосных станций, мониторинг состояния магистральных и промысловых газо- и нефтепроводов.

Клиентами МЦ являются физические и юридические лица. Для занесения данных о клиенте в базу данных МЦ используются средства АС. Также, в рамках исполнения требований Трудового кодекса РФ в АС, допускается обработка персональных данных (ПДн) сотрудников.

Для обеспечения безопасности персональных данных используются методы, которые условно можно разделить на три категории:

— правовые методы [1–8];

— организационные методы;

— технические или инженерно-технические методы.

В рамках поставленной задачи — обеспечение ИБ ПДн, было произведено обследование и ознакомление со структурой отдельного МЦ. В процессе обследования МЦ была определена его организационная структура, представленная на рис. 1.

Всего в организации шесть департаментов:

— департамент продаж;

— департамент государственных и ведомственных проектов;

— департамент обслуживания клиентов;

— департамент оперативного реагирования;

— технический департамент;

— департамент бухгалтерского и налогового учета.

Каждый департамент возглавляет директор. Наряду с этим в организации есть восемь отдельных подразделений, не входящих в состав департаментов:

— сервисный центр;

— юридическая служба;

— ведущий менеджер по рекламе и PR;

— служба безопасности;

— служба персонала;

— отдел обслуживания корпоративных клиентов;

— административно-хозяйственная служба;

— менеджер по работе со страховыми компаниями.

Штатная численность организации более 500 человек. Во главе организации — генеральный директор. График работы для отдела обслуживания клиентов, оперативно-дежурной службы, call-центра, отдела эксплуатации и развития технической сети установлен круглосуточный, без выходных. Остальные отделы работают в будние дни с 09:00 до 17:00.

Здание офиса МЦ, где расположена АС, трехэтажное, кирпично-монолитное. Межэтажные перекрытия из керамзитобетона, в качестве покрытия потолка используется технология фальшпотолок, внутри которого достаточно много свободного пространства, где проведена проводка, кабели и слаботочные сети.

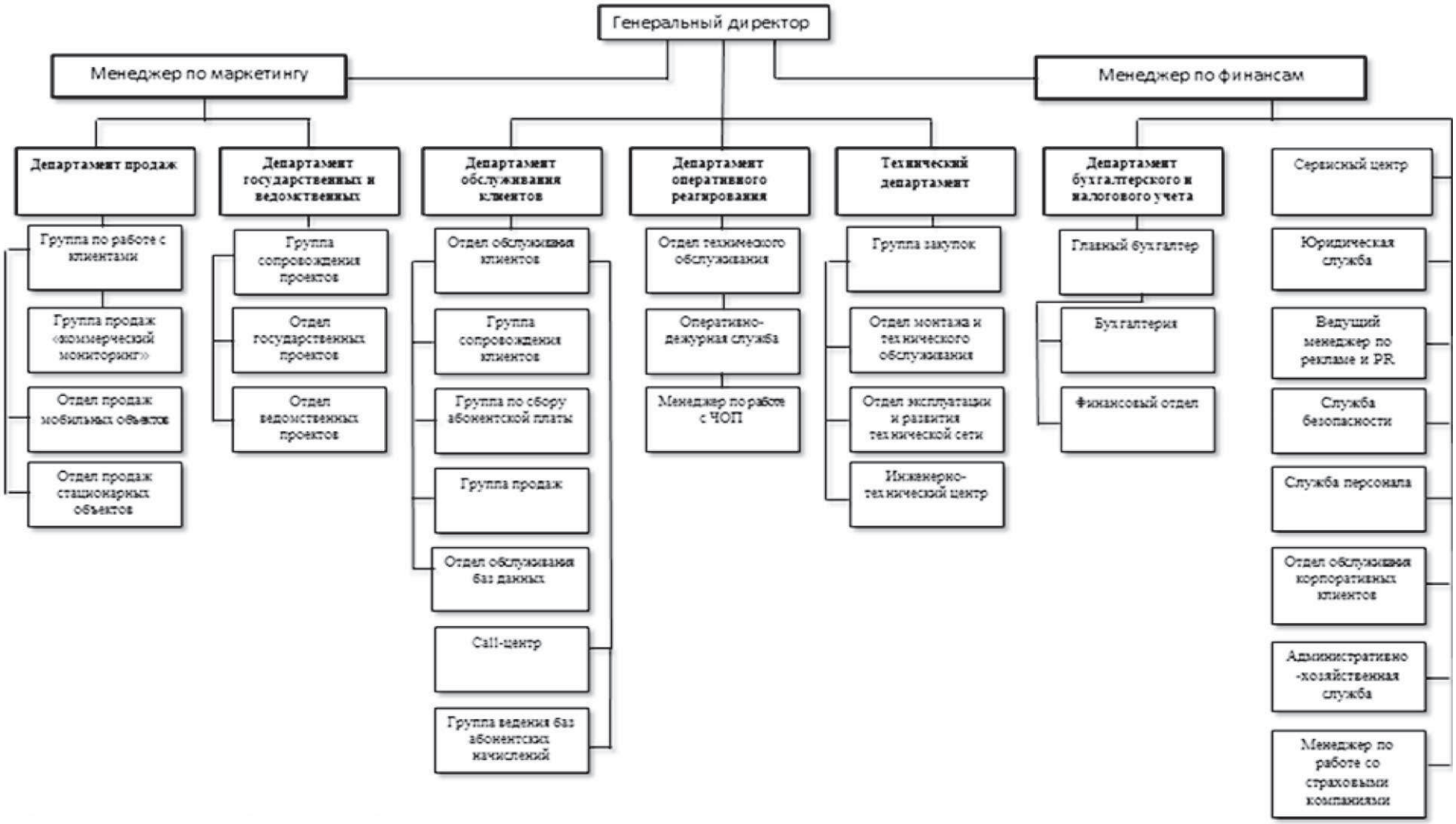

Рис. 1. Структура мониторингового центра

В предпроектном обследовании, был проведен анализ работы исходной АС МЦ. При построении схемы размещения основных технических средств и систем (далее — ОТСС) с привязкой к границе контролируемой зоны была проведена полная инвентаризация автоматизированных рабочих мест (далее — АРМ) и серверного оборудования (рис. 2).

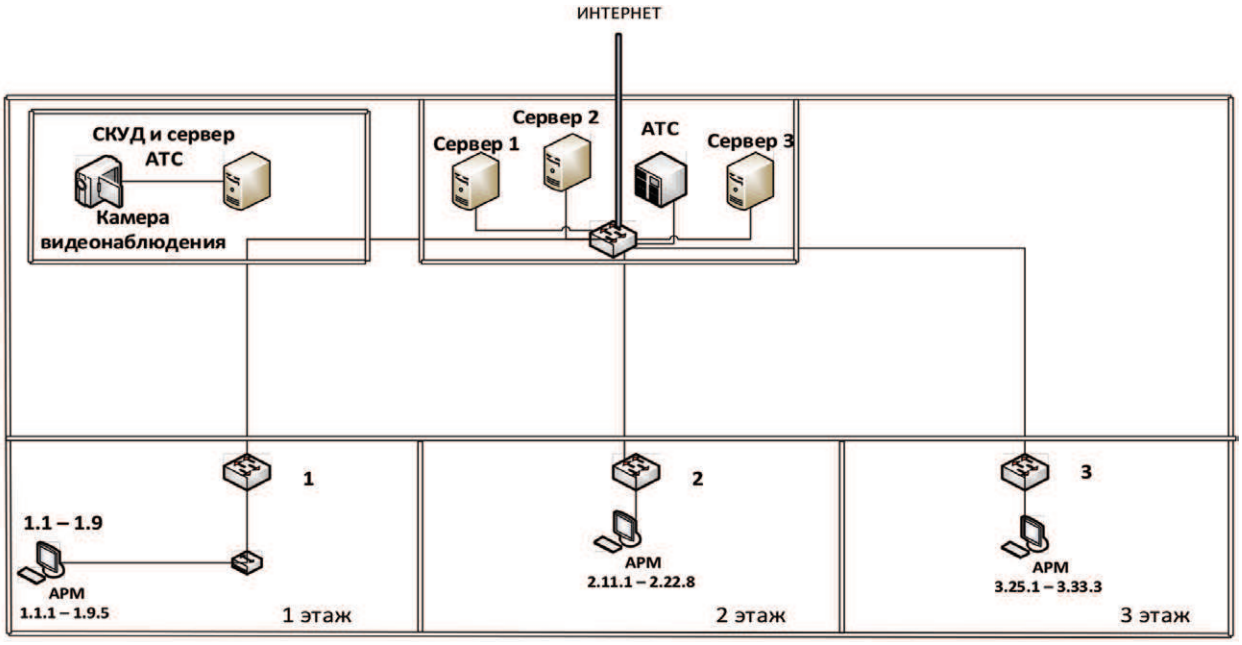

Рис. 2. Схема логики работы АС в незащищенном исполнении

На вышеуказанной схеме также показан канал организации работы с информационно-коммуникационной сетью Интернет. Доступ к Сети организован при помощи коммутационного оборудования. Межсетевой экран не используется.

АРМы объединены в единую АС посредством коммутаторов и имеют типовую структуру и конфигурацию.

Для размещения коммутационного оборудования в коридорах здания МЦ используют стандартные настенные коммуникационные шкафы (далее — КШ) с присоединительными размерами в 19 дюймов. Нумерация шкафов произведена в соответствии с номером этажа. От КШ сетевой кабель идет в управляемый коммутатор, который расположен в каждом кабинете. На каждом коммутаторе имеются 24 программируемых порта.

В МЦ используется комбинированная сетевая топология расширенной звезды. В таком варианте выход из строя одного АРМ никак не повлияет на работу сети, остальные АРМ по-прежнему взаимодействуют друг с другом.

Всего в АС используются 8 серверов, более 130 АРМ, 32 коммутатора и 3 КШ. Сетевые розетки опломбированы и пронумерованы. На серверах, являющихся продукцией компании HP, установлена лицензионная серверная операционная система семейства Microsoft. Базовая операционной системы для АРМов — Microsoft Windows 7 Professional. В АС МЦ используется типовое программное обеспечение (1С, Microsoft Office, Rander, программные средства собственной разработки и др.), установка и настройка которого производится строго в соответствии с определенным регламентом.

В АС обрабатывается как общедоступная информация, так и информация ограниченного доступа. К информации ограниченного доступа МЦ относится:

— коммерческая тайна [3];

— ПДн клиентов;

— ПДн сотрудников [5–8].

После проведенного анализа работы подразделений с сегментами было установлено, какие подразделения работают с ПДн клиентов:

— группа по работе с клиентами;
— группа продаж «коммерческий мониторинг»;
— отдел продаж мобильных объектов;
— отдел продаж стационарных объектов;
— отдел обслуживания клиентов;
— группа сопровождения клиентов;
— группа по сбору абонентской платы;
— отдел обслуживания баз данных;
— call-центр;
— группа ведения баз абонентских начислений;
— отдел технического обслуживания;
— оперативно-дежурная группа.

С ПДн сотрудников работают:

— главный бухгалтер;
— бухгалтерия;
— служба безопасности;
— служба персонала;
— менеджер по работе со страховыми компаниями.

Исходя из вышеизложенного, можно сделать вывод: практически во всех информационных подсистемах МЦ обрабатываются ПДн сотрудников и клиентов компании. Наряду с этим данные подсистемы имеют постоянный выход в Интернет и физически неразрывны друг с другом.

Схема информационных потоков ПДн между департаментами, обрабатывающими ПДн, представлена на рис. 3.

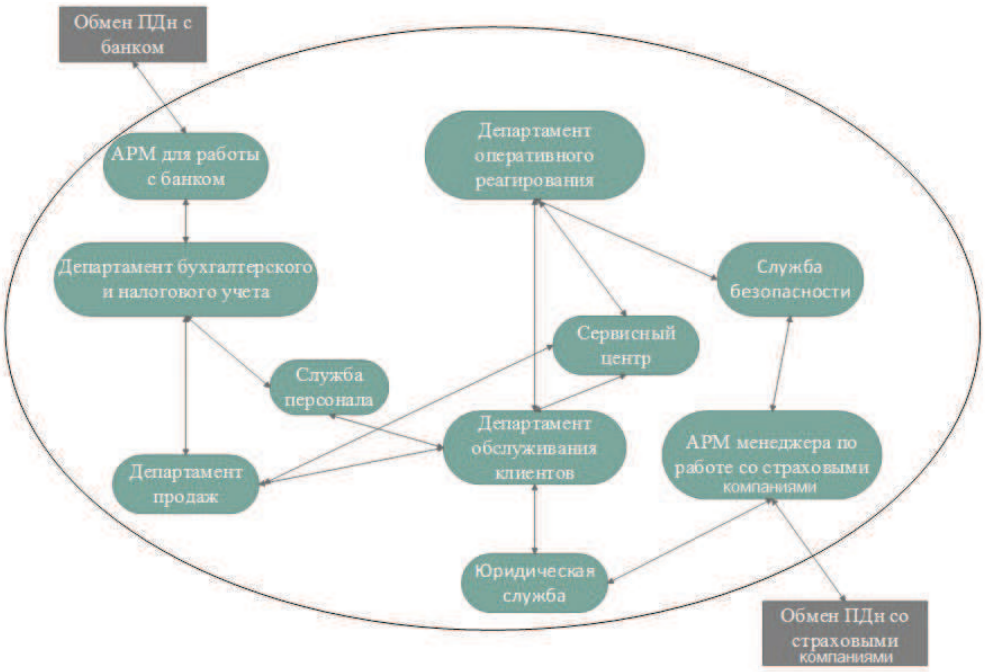

Рис. 3. Схема информационных потоков персональных данных между департаментами, обрабатывающими персональные данные

При проектировании системы защиты ИСПДн МЦ необходимо провести комплекс работ, включающий в себя:

— правовую защиту;

— организационную защиту;

— техническую защиту.

При анализе нормативно-правовой базы было установлено, что для Российской Федерации при проведении работ по построению защиты ИСПДн МЦ оказания телематических услуг безопасности в защищенном исполнении следует руководствоваться следующей нормативно-правовой базой:

1) Конституция РФ (ст. 24);

2) Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

3) Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;

4) Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

5) Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

6) Постановление Правительства РФ от 6 июля 2008 г. № 512 (ред. от 27 декабря 2012 г.) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне ИСПДн»;

7) Постановление правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

8) Приказ Федеральной службы технического и экспортного контроля России № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Детальное изучение вышеуказанной нормативно-правовой базы позволяет построить перечень минимальных организационно-правовых мер, которые необходимо выполнить оператору, в нашем случае МЦ, чтобы выполнить требования законодателя. При определении требований, исходя из того, что оператор находится на территории Российской Федерации и трансграничную передачу данных не осуществляет, были разработаны следующие документы:

1) Акт классификации информационной системы персональных данных;

2) Определение границ контролируемой зоны;

3) Технический паспорт ИСПДн;

4) Регламент разграничения прав доступа к ПДн;

5) Приказ о назначении администратора безопасности ИСПДн;

6) Руководство администратора ИСПДн;

7) Руководство пользователя ИСПДн;

8) Приказ об утверждении списка лиц, которым необходим доступ к ПДн, обрабатываемым в ИСПДн, для выполнения служебных обязанностей;

9) Перечень применяемых средств защиты информации;

10) Перечень эксплуатационной и технической документации применяемых СЗИ;

11) Перечень носителей ПДн;

12) Положение о защите ПДн;

13) Положение об организации режима безопасности помещений, где осуществляется работа с ПДн;

14) Положение о порядке хранения и уничтожения носителей ПДн.

С целью определения требований к защите ПДн при их обработке в ИС ПДн необходимо определить уровень защищенности ПДн. Для этого нужно обратиться к Постановлению Правительства от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», определяющего уровни защищенности ПДн. Сначала следует определить категорию обрабатываемых данных. Для ка-

тегорирования необходимо установить, какие именного данные обрабатываются в случае, когда в АС МЦ используются ПДн сотрудников, а какие в случае использования ПДн клиентов.

К ПДн сотрудников отнесли: Ф. И. О.; паспортные данные; контактные данные; данные, необходимые для работы бухгалтерии; данные, необходимые для работы кадровой службы, в том числе сведения о состоянии здоровья; данные, необходимые для работы внутренней службы безопасности.

К ПДн клиентов отнесли Ф. И. О.; паспортные данные; контактные данные.

Исходя из этого, установлено, что в информационной системе персональных данных мониторингового центра обрабатываются ПДн трех видов: специальные, биометрические и иные категории персональных данных.

Следующим шагом устанавливаются угрозы ИСПДн МЦ. На основе пп. 1119 ч. 6 пришли к заключению, что для информационной системы персональных данных актуальны угрозы второго типа.

Далее определили класс защищенности АС: пп. 1119 ч. 10 (б, в, д), указывает, что ИСПДн мониторингового центра имеет необходимость второго уровня защищенности. Далее на представленной табл. 1 показана краткая характеристика обрабатываемых ПДн.

Таблица 1

Классификация и требования по защите

<table>
<tr><td colspan="2" rowspan="2">Нормативный документ</td><td colspan="2">ИСПДн МЦ</td></tr>
<tr><td>ПДн сотрудников < 1000</td><td>ПДн клиентов > 100 000</td></tr>
<tr><td rowspan="2">Категории ПДн</td><td>пп. 1119 ч. 5</td><td>Специальные категории ПДн</td><td>Иные ПДн</td></tr>
<tr><td>пп. 1119 ч. 5</td><td>Биометрические ПДн</td><td></td></tr>
<tr><td>Тип угрозы</td><td>пп. 1119 ч. 6</td><td colspan="2">Угрозы второго типа</td></tr>
<tr><td>Уровень защищенности</td><td>пп. 1119 ч. 10 (б, в, д)
пп. 1119 ч. 15</td><td colspan="2">Необходимость второго уровня защищенности</td></tr>
<tr><td rowspan="4">Требования безопасности</td><td rowspan="4">Приказ ФСТЭК № 21</td><td>СВТ</td><td>Не ниже 5-го класса</td></tr>
<tr><td>Системы обнаружения вторжений</td><td>Не ниже 4-го класса</td></tr>
<tr><td>Средства антивирусной защиты</td><td>Не ниже 4-го класса</td></tr>
<tr><td>Межсетевой экран</td><td>Не ниже 3-го класса</td></tr>
</table>

Стоит обратить внимание на то, что персонал обрабатывает ПДн субъектов согласно своим должностным инструкциям. Полный доступ к информации конфиденциального характера имеют директор, начальник службы безопасности и специалист по защите информации на предприятии.

Теперь стоит уделить внимание техническим мероприятиям по обеспечению конфиденциальности информации в процессе проектирования объекта информатизации.

Основополагающим документом служит приказ ФСТЭК 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». В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

— идентификация и аутентификация субъектов доступа и объектов доступа;

— управление доступом субъектов доступа к объектам доступа;

— ограничение программной среды;

— защита машинных носителей информации, на которых хранятся и/или обрабатываются персональные данные (далее — машинные носители персональных данных);

— регистрация событий безопасности;

— антивирусная защита;

— обнаружение (предотвращение) вторжений;

— контроль (анализ) защищенности персональных данных;

— обеспечение целостности информационной системы и персональных данных;

— обеспечение доступности персональных данных;

— защита среды виртуализации;

— защита технических средств;

— защита информационной системы, ее средств, систем связи и передачи данных;

— выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и/или к возникновению угроз безопасности персональных данных (далее — инциденты), и реагирование на них;

— управление конфигурацией информационной системы и системы защиты персональных данных.

Дополнительно согласно ч. 11. Приказа № 21 ФСТЭК России:

— проверка системного и/или прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и/или без использования таковых;

— тестирование информационной системы на проникновения;

— использование в информационной системе системного и/или прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

Для второго уровня защищенности предусмотрены 69 минимальных мер.

Согласно ч. 12 Приказа № 21 ФСТЭК России при использовании в информационных системах, сертифицированных по требованиям безопасности информации средств защиты информации, для обеспечения 1-го и 2-го уровней защищенности ПДн:

— средства вычислительной техники не ниже 5-го класса по уровню недекларированных возможностей;

— системы обнаружения вторжений и средства антивирусной защиты не ниже 4-го класса;

— межсетевые экраны не ниже 3-го класса.

В дополнение к вышесказанному, для обеспечения 1-го и 2-го уровней защищенности персональных данных, а также для обеспечения 3-го уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы второго типа, применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4-му уровню контроля отсутствия недекларированных возможностей.

В результате анализа всех функциональных возможностей программных средств среди средств обнаружения и предотвращения вторжений было выбрано СОВ фирмы «Рубикон». В состав данного комплекса входит маршрутизатор с поддержкой мандатных меток, построение однонаправленных шлюзов, функционал обнаружения атак по протоколам сетевого, транспортного уровня и уровня приложений, трансляции сетевых адресов. Количество сетевых портов — от 6 до 64, в том числе и оптических. Так как в его состав входит межсетевой экран, который отвечает всем требованиям по обеспечению безопасности 1-го и 2-го уровней защищенности, нам не нужно искать ему замену.

При анализе средств антивирусной защиты по требованиям приказа № 21 ФСТЭК России был выбран Антивирус Касперского Endpoint Security 10 для Windows. Он отвечает всем требованиям, описанным в руководящем документе «Антивирусные средства, показатели защищенности и требования по защите антивирусов».

В результате применения технических средств защиты информации схема логики работы АС видоизменилась (рис. 4). После применения ТСЗИ получилось следующее:

— доступ к автоматизированной системе извне фильтруется межсетевым экраном [10];

— коммуникационные шкафы делят на сектора внутреннюю информационную среду, тем самым распределяя потоки данных;

— сформирована серверная комната 9, куда добавлены 8 серверов: сервер приложений, сервер электронной почты, сервер БД клиентов, сервер БД сотрудников, сервер управления, сервер СКУД, прокси-сервер, FTP-сервер;

— подключены дополнительные коммуникаторы для работы с ПДн и для работы с коммерческой информацией;

— добавлен распределительный коммуникатор, для экономии портов МЭ;

— отдельно выделены АРМы для работы с банком и страховыми компаниями;

— всего в АС МЦ 122 АРМ, из них на первом этаже располагается 38, на втором — 62 и на третьем — 22.

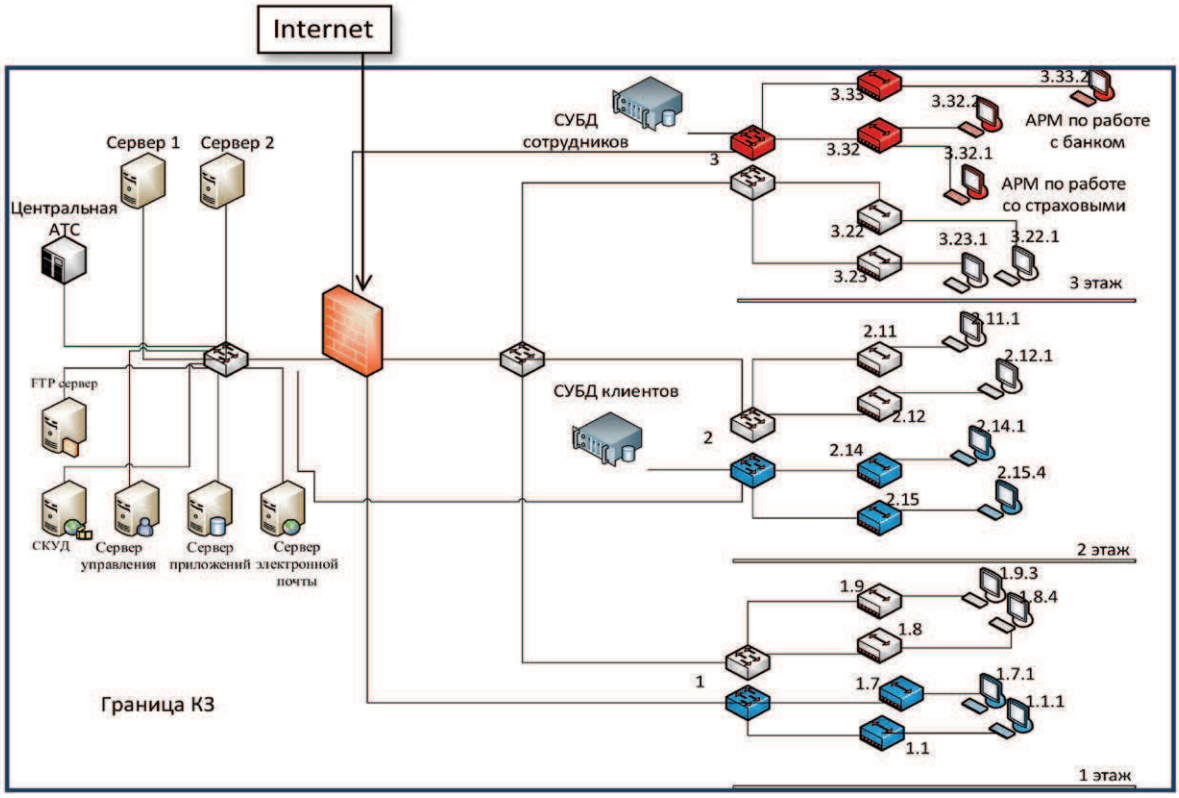

Рис. 4. Видоизмененная схема логики работы АС

Для реализации организационных мер необходимо создать отдел информационной безопасности, в обязанности сотрудников которого согласно должностной инструкции будет входить:

1) проведение организационно-технических мероприятий, разработка методических и нормативных документов, проведение плановых обновлений;

2) сбор и анализ материалов о возможных каналах утечки информации, в том числе по техническим каналам;

3) анализ существующих методов и средств, применяемых для контроля и защиты информации, и разработка предложений по их совершенствованию и повышению эффективности защиты;

4) обследование объектов защиты, их аттестация и категорирование;

5) определение потребностей в ТСЗИ и мониторинг результатов их внедрения.

Перед вводом ИСПДн МЦ в эксплуатацию нужно решить вопрос технического соответствия требованиям регуляторов РФ. Есть два решения: аттестация соответствия и декларация соответствия [9].

Аттестация **ИСПДн** относится только к государственным информационным системам персональных данных, что накладывает на операторов обязательства по их защите в соответствии с «Требованиями по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными Приказом ФСТЭК России № 17 от 11 февраля 2013 г. Так как МЦ — коммерческая организация, то процедура аттестации носит необязательный характер.

Декларирование соответствия — это документальное подтверждение соответствия свойств и характеристик ИСПДн, предъявляемым к ней требованиям, которые установлены законодательством РФ о персональных данных, а также нормативными и методическими документами Роскомнадзора, ФСТЭК России и ФСБ России. Декларирование является одной из форм подтверждения соответствия наряду с аттестацией ИСПДн.

На сегодняшний момент процедура декларирования коммерческих ИСПДн не регламентирована и, так же как и процедура аттестации соответствия, является добровольной процедурой.

Подводя итоги, необходимо отметить, что комплекс мер по защите информационной системы персональных данных носит рекомендательный характер и может быть изменен, в соответствии с предпочтениями руководства.

Предложенный набор организационных и технических мер не является исчерпывающим, а представляет собой минимальный комплекс, который отвечает нормативным требованиям.

Список литературы

1. Конституция РФ. Ст. 24.

2. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных: федеральный закон Рос. Федерации от 19 декабря 2005 г. № 160-ФЗ.

3. О коммерческой тайне: федеральный закон Рос. Федерации от 29 июля 2004 г. № 98-ФЗ.

4. Об информации, информационных технологиях и о защите информации: федеральный закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ.

5. О персональных данных: федеральный закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ.

6. Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне ИСПДн: Постановление Правительства Рос. Федерации от 6 июля 2008 г. № 512 (в ред. от 27 декабря 2012 г.).

7. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства Рос. Федерации от 1 ноября 2012 г. № 1119.

8. Об утверждении Состава и содержания технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ Федеральной службы технического и экспортного контроля России от 18 февраля 2013 г. № 21.

9. Автоматизация и информационные технологии — от постановки до ввода в эксплуатацию: моногр. / В. В. Аникин, Р. Ш. Аюпов [и др.]. — Одесса: Изд-во «Куприенко Сергей Васильевич», 2013.

10. *Ныркова А. П.* Помехозащищенность как фактор обеспечения стабильной работы сети передачи данных на транспорте / А. П. Ныркова, С. С. Соколов, А. С. Белоусов // Sworld: сб. науч. тр. — 2013. — Т. 8, № 1. — С. 5–9.