

**Я. И. ГУЛИЕВ,**

к.т.н., руководитель Исследовательского центра медицинской информатики
Института программных систем им. А.К. Айламазяна РАН,
г. Переславль-Залесский, Ярославская обл., Россия, yag@interin.ru

А. А. ЦВЕТКОВ,

научный сотрудник Исследовательского центра медицинской информатики
Института программных систем им. А.К. Айламазяна РАН,
г. Переславль-Залесский, Ярославская обл., Россия, sio@interin.com

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МЕДИЦИНСКИХ ОРГАНИЗАЦИЯХ

УДК 004.7.056.53

Гулиев Я.И., Цветков А.А. *Обеспечение информационной безопасности в медицинских организациях (Институт программных систем им. А.К. Айламазяна РАН)*

Аннотация. В статье рассматриваются вопросы защиты персональных данных в медицинских организациях в соответствии с требованиями законодательства и нормативных документов регуляторов Российской Федерации, обсуждаются актуальные угрозы информационной безопасности, которые характерны для медицинских информационных систем. Предложены необходимые меры, которые должны обеспечить информационную безопасность, включая модель архитектуры защищенной информационной среды медицинской организации.

Ключевые слова: защита персональных данных, медицинская организация, законодательство, нормативные документы, угрозы информационной безопасности, информационная среда медицинской организации, медицинская информационная система, инциденты информационной безопасности.

UDC 004.7.056.53

Guliev Y.I., Tsvetkov A.A. *Ensuring Information Security in Healthcare Organizations (Ailamazyan Program Systems Institute of RAS)*

Abstract. The article addresses issues of protection of personal data in medical organizations in accordance with the laws and regulations of the Russian Federation regulators, discussing topical information security threats that are specific to medical information systems. We propose the necessary actions to ensure information security, including secure information architecture model among healthcare organizations.

Keywords: protection of personal data, medical organization, legislation, normative documents, information security threats, information environment of the medical organization, medical information system, information security incidents.

ВВЕДЕНИЕ

В настоящее время проблемам информационной безопасности (далее ИБ) придается особое внимание на самом высоком государственном уровне. Подтверждением этого является появление в 2000 году документа «Доктрина информационной безопасности Российской Федерации» [1]. Согласно Доктрине, «Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».



Конкретизация требований Доктрины и особенностей ее применения привели к появлению ряда законодательных, нормативных и рекомендательных документов (см. [2] ... [8]).

В частности, интересы личности в информационной сфере определяются в Федеральном законе от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» [2], в котором вводятся все основные термины и определения, связанные с персональными данными (далее ПДн), устанавливается требование о необходимости защиты ПДн и перечисляются обязательные меры для выполнения этого требования.

В законе «О персональных данных» упоминаются различные типы информационных систем (далее ИС), статус которых должен быть установлен законодательно. В Федеральном законе от 27.07.2006 № 149-ФЗ (ред. от 06.07.2016) «Об информации, информационных технологиях и о защите информации» [4] статус ИС формулируется и содержит три типа ИС:

- Государственные ИС;
- Муниципальные ИС;
- Иные ИС.

Для медицинских организаций (далее МО), поскольку лечебные и вспомогательные процессы связаны с обработкой информации о пациентах, которая хранится на традиционных носителях («бумажные» документы) или в цифровом виде в медицинских информационных системах (далее МИС), защита информации является важным и обязательным требованием. При этом в МИС, как правило, не обрабатывается информация, связанная с государственной тайной или формированием законодательных актов на государственном или муниципальном уровнях, т.е. МИС относится к типу «Иные информационные системы». В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» [4]:

«Порядок создания и эксплуатации информационных систем, не являющихся госу-

дарственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами».

В статье рассматриваются проблемы ИБ в МО, в которых информация обрабатывается в цифровом виде в МИС.

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОТ ТРЕБОВАНИЙ К РЕАЛИЗАЦИИ

В «Доктрине информационной безопасности Российской Федерации» содержится требование «обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством», которое является одним из основных национальных интересов Российской Федерации в информационной сфере. Но раскрытие этого понятия, а именно «персональные данные», осуществляется в Федеральном законе № 152-ФЗ «О персональных данных» [2]:

«персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)».

В Федеральном законе «О персональных данных» [2] также вводятся следующие определения, которые авторы используют в настоящей работе:

- *«оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия*



Рис. 1. Законодательная, нормативная и справочная документация по ИБ

(операции), совершаемые с персональными данными»;

- «обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных»;
- «автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники»;
- «информационная система персональных данных – совокупность содержащихся в базах

данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств».

Кроме того, в Федеральном законе «О персональных данных» вводится понятие «Специальные категории персональных данных», т.е. ПДн, которые касаются «расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни».

Исходя из этого, в настоящей статье под МИС понимается следующее:

медицинская информационная система – это информационная система персональных данных, которая содержит специальные категории персональных данных о состоянии здоровья.

На МО как оператора ПДн, согласно Федеральному закону «О персональных данных», налагается следующее требование:





«Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных».

Это должно достигаться [2]:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных дан-

ных и уровня защищенности информационных систем персональных данных.

Следует дополнить, что для МИС необходимым требованием является соблюдение врачебной тайны (см. [6]).

Эти декларативные требования расширяются и поясняются в ряде документов, принятых Правительством Российской Федерации и Федеральной службой по техническому и экспортному контролю России (далее ФСТЭК России) ([3], [5], [7], [8]).

В [3] дается подробное описание того, как оценить требуемый уровень защищенности (далее УЗ) МИС. А в [9] приводятся практические рекомендации по определению необходимого УЗ. Согласно [9], следует считать, что, если количество субъектов, ПДн которых обрабатываются в МИС менее 100 тысяч, то необходимо обеспечить в МИС 3-й УЗ, а если количество субъектов ПДн более 100 тысяч, то необходимо обеспечить 2-ой УЗ.

Следует отметить, что очень часто по разным причинам операторы ПДн, обрабатываемых в МИС, пытаются классифицировать свои ИСПДн как системы, которые предполагают 1-й УЗ. Однако, это неверно в большинстве случаев (по крайней мере для муниципальных и частных МО), т.к. 1-й УЗ относится, как правило, к государственным информационным системам (далее ГИС), т.е. информационным системам (далее ИС), содержащим документы с государственной тайной. Почти все, возможно за редким исключением, МО в своих МИС не обрабатывают информацию, содержащую государственную тайну. В то же время, оператор ПДн может (имеет право) принять решение о том, чтобы его МИС классифицировалась по 1-му УЗ, но при этом стоимость средств защиты ПДн возрастает в разы.

В [5] перечисляются меры по обеспечению различных УЗ, а в [8] даются рекомендации по организации этих мер.

Конечной задачей, которая решается в процессе выполнения требований законода-



тельных и нормативных документов, является задача выявления актуальных для эксплуатируемой/создаваемой МИС угроз и уязвимостей, которые в ней существуют, с последующей нейтрализацией этих угроз за счет создания/модернизации системы ИБ в МО (см. Рис. 2).

Из рисунка видно, что процессы обеспечения ИБ в МО являются непростой задачей, и качество обеспечения ИБ определяется еще на предварительных этапах: анализ законодательной и нормативно-справочной информации по защите ПДн, разработка частной модели угроз, конкретизация мер ФСТЭК России по защите ПДн. Конечным результатом этих этапов будет техническое задание на разработку и создание системы ИБ в МО, которая, в частности, обеспечит безопасность ПДн.

Следует дополнительно отметить, что согласно Федеральному закону «О персональных данных» [2], «оператор при обработке персональных данных обязан принимать необ-

ходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных». Т.е. руководитель МО является лицом, ответственным за выполнение требований законодательства РФ, а в случае их нарушения несет за это персональную ответственность.

В то же время, существует определенный порядок, согласно которому, организация, уполномоченная ФСТЭК России, может при обращении к ней провести аттестацию ИС МО на соответствие требованиям законодательства РФ в области защиты ПДн. При наличии такого аттестата вся ответственность за возникновение инцидента, связанного с ИБ, ложится на организацию, которая аттестовала ИСПДн.

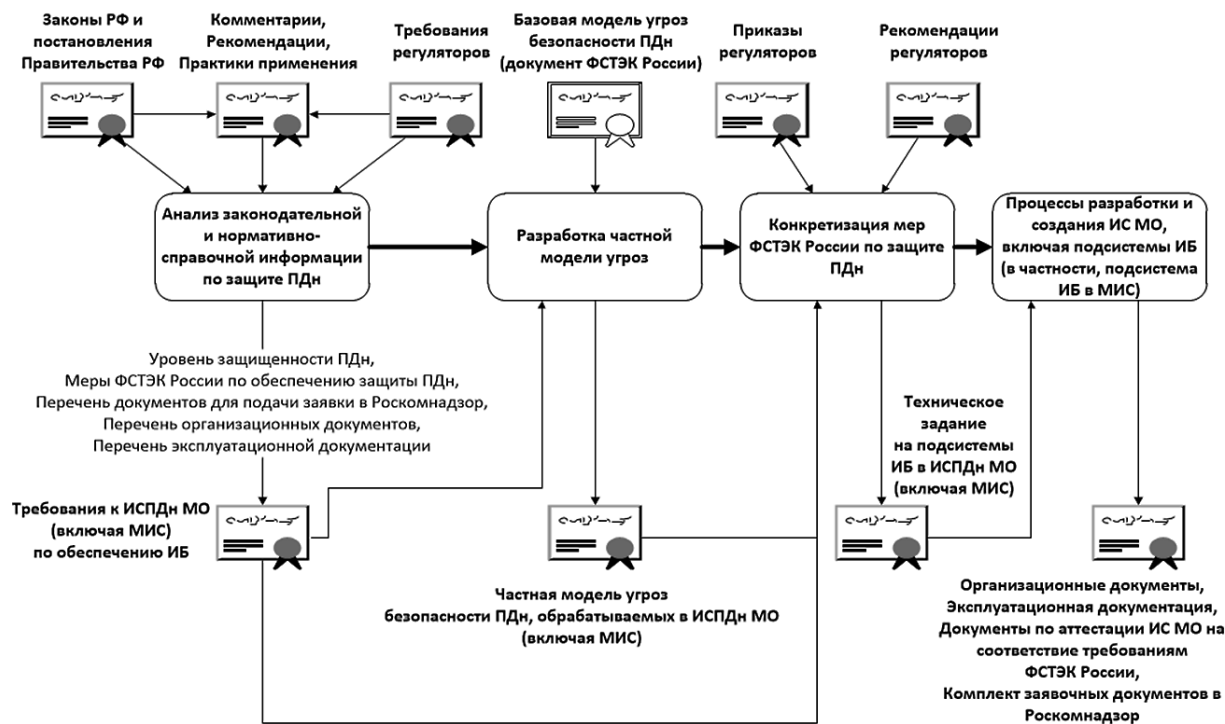


Рис. 2. Процессы обеспечения ИБ (в частности, защиты ПДн)





2. АКТУАЛЬНЫЕ УГРОЗЫ ИБ И ВОЗМОЖНОСТЬ ИХ РЕАЛИЗАЦИИ В ИСПДН

Выше неоднократно упоминались такие понятия, как «угрозы» и «уязвимости». Среди неспециалистов в области ИБ существует определенная путаница в трактовке этих понятий. Однако, существуют определения того, что следует понимать под «угрозой» и «уязвимостью» (см. [7]).

«Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных».

«Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации».

Согласно [7], угрозы безопасности ПДн делятся на два основных типа: угрозы утечки информации по техническим каналам и угрозы несанкционированного доступа к информации в ИСПДн.

Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.

Угрозы несанкционированного доступа к информации в ИСПДн включают в себя:

- угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);

- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;

- угрозы внедрения вредоносных программ (программно-математического воздействия).

Однако, в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» [4], для ИСПДн, используемых в МО (включая МИС), угрозы утечки информации по техническим каналам и угрозы, связанные с закладками в операционной системе (далее ОС) или прикладном программном обеспечении (далее ПО), не считаются актуальными. В соответствии с этим же законом, такие ИСПДн следует классифицировать как относящиеся ко 2-му или 3-му УЗ.

В ряде разъяснений, которые давали в ФСТЭК России, это объясняется принципом соизмеримости стоимости информационного актива (в данном случае это ПДн пациентов) и возможных потерь от утраты/модификации данных со стоимостью средств защиты информации (далее СЗИ) от несанкционированного

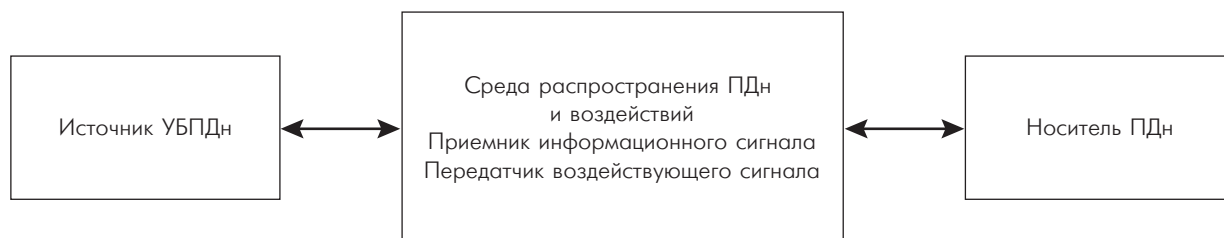


Рис. 3. Обобщенная схема канала реализации угроз безопасности ПДн [7]



доступа (далее НСД). Действительно, как показывает опыт, получение НСД к ИСПДн через уязвимости ОС или уязвимости прикладного ПО требует серьезных ресурсов, в том числе привлечения высококвалифицированных коллективов специалистов.

Анализ типовой МО показывает, что актуальными угрозами безопасности ПДн для нее являются:

- угрозы от действий вредоносных программ (вирусов);
- угрозы утраты ключей и атрибутов доступа.

Минимальными рекомендуемыми мерами по предотвращению реализации актуальных угроз, которые перечисляются в частной модели угроз, являются:

- установка антивирусной защиты;
- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;
- назначение ответственного за безопасность персональных данных из числа сотрудников учреждения;
- разработка инструкций пользователей ИСПДн, в которых должны быть отражены правила безопасной работы с ИСПДн, а также правила работы с ключами и атрибутами доступа.

Следует заметить, что перечисленные актуальные угрозы и минимальные рекомендуемые меры по их нейтрализации являются достаточными для разработки документа «Частная модель угроз», который является обязательным для подачи в составе комплекта документов в Роскомнадзор для уведомления об обработке ПДн в МО.

Кроме того, должны быть обеспечены требования Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [5]:

- 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.

3. ТИПОВАЯ АРХИТЕКТУРА ЗАЩИЩЕННОЙ МИС В МО

Существует множество документов, в которых перечисляются возможные угрозы и уязвимости ИСПДн, даются рекомендации по устранению недостатков в обеспечении ИБ (например, [5], [6], [7], [8]). Но они не отвечают на вопрос: «Что нужно конкретно для Вашей ИСПДн?»

В этом разделе опишем модель защиты, основанную на наиболее распространен-



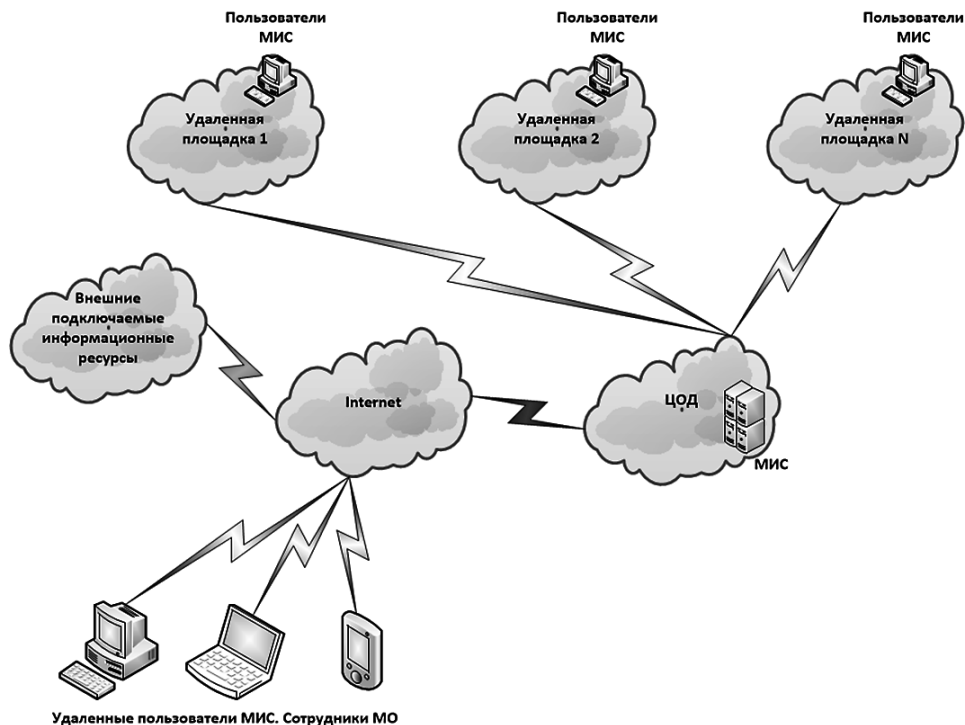


Рис. 4. Обобщенная архитектура ИС МО. До анализа состояния ИБ

ных, проверенных и доступных средствах. Для определенности рассмотрим некоторую обобщенную архитектуру ИС МО, в которой ПДн обрабатывает МИС (см. Рис. 4).

Предполагается, что ИС МО включает в себя:

- центр обработки данных (далее ЦОД);
- несколько удаленных площадок, которые подключены к ЦОД по доверенным каналам связи;
- удаленные пользователи МИС, которые являются сотрудниками МО и которые подключаются к МИС посредством сети общего доступа (Internet);
- внешние подключаемые информационные ресурсы, с которыми могут взаимодействовать пользователи МИС или непосредственно сама МИС (передача отчетов, обновления от разработчика, обновления справочников, прием запросов и др. обмен данными, регламентированными документами

органов здравоохранения общероссийского и местного уровней).

Особенности каждой МО невозможно учесть, и в каждом конкретном случае необходим тщательный анализ возможных угроз и уязвимостей, которые могут привести к дискредитации всей системы и хранящихся в ней информационных активов, включая ПДн. Но решения по предотвращению угроз для некоторой «усредненной» МО, которая рассматривалась в данной статье, можно представить в виде модели, показанной на Рис. 5.

Будем считать, что в МО используется централизованное размещение серверов, образующих логическую структуру всей ИСПДн и содержащих непосредственно саму ИСПДн в ЦОД, который связан с операторами МИС (сотрудниками МО) через локальную вычислительную сеть (далее ЛВС), доверенные каналы связи с удаленными площадками МО,

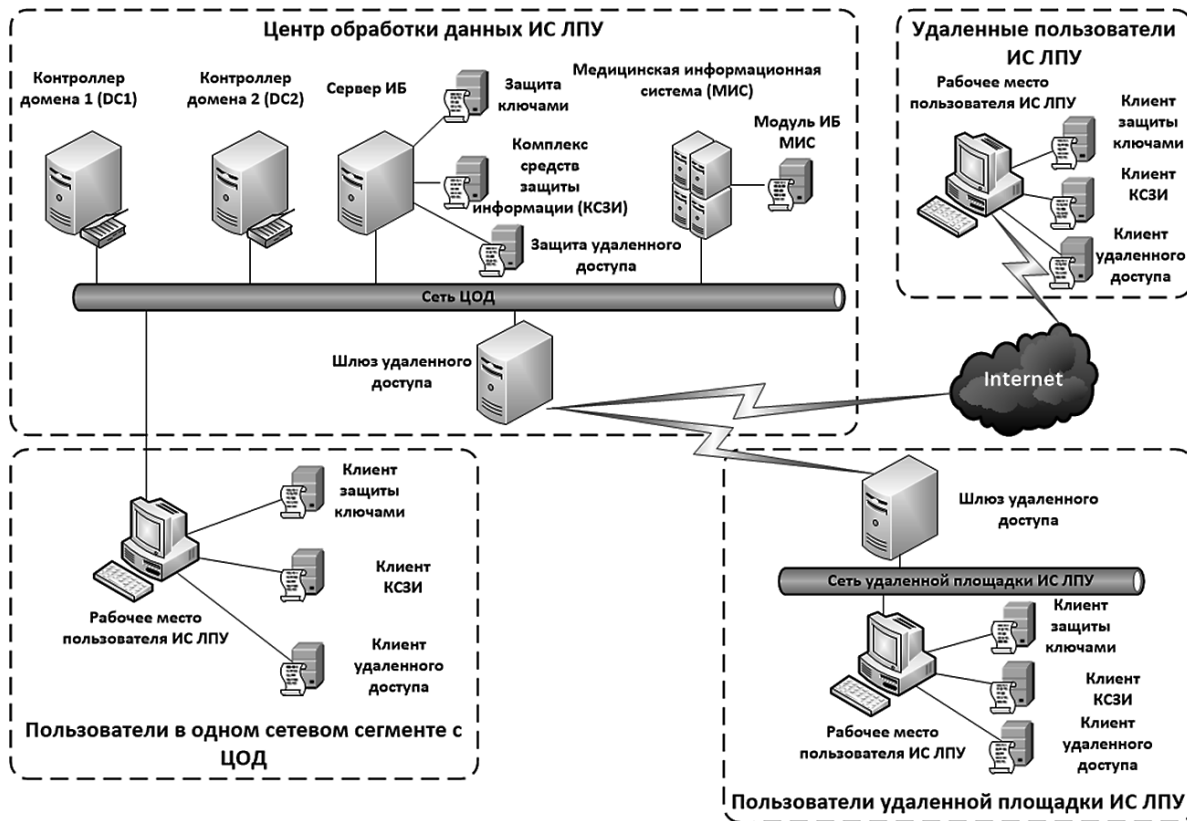


Рис. 5. Модель мер по защите ПДн в МО

каналы связи Internet. Описание элементов модели мер по защите ПДн в МО приводится в Табл. 1.

В этой модели система защиты строится на основе:

- комплексной системы защиты информации (КСЗИ);
- системы защиты ключами;
- системы защиты удаленного доступа;
- шлюза удаленного доступа.

КСЗИ решает следующие задачи:

- Для каждого внутреннего пользователя МО создается число учетных записей (для входа в систему они используют один пароль), по числу ролей, где каждая роль предполагает выполнение определенных обязанностей с соответствующими ограничениями (например, работа с МИС, обработка кон-

фиденциальных документов определенными приложениями, работа в сети Internet и т.д.).

- Для каждой роли (каждой учетной записи) устанавливаются соответствующие разграничения прав доступа к файловым объектам, внешним накопителям, сетевым ресурсам, принтерам и т.д., с учетом политики МО по обработке защищаемой информации.

- Полностью изолируется обработка информации в различных режимах (для различных ролей сотрудника).

КСЗИ состоит из сервера КСЗИ и клиента, который обеспечивает взаимодействие рабочего места пользователя ИС МО с сервером КСЗИ.

Система защиты ключами состоит из:









- сервера защиты ключами, который решает задачу аутентификации пользователей











Табл. 1.

Описание элементов модели мер по защите ПДн в МО

<i>Элемент модели мер по защите</i>	<i>Описание элемента</i>
<p>Контроллер домена 1 (DC1)</p> 	<p>Серверы, образующие логическую структуру информационной среды: корневой домен, дочерние домены, пользователи и их права в информационной среде. В частности, право подключения к различным ИСПДн, например, к МИС. Часть сервисов доменных контроллеров используется для работы ПО, обеспечивающего ИБ</p>
<p>Медицинская информационная система (МИС)</p> 	<p>Сервер приложений, который включает в себя МИС</p>
<p>Модуль ИБ МИС</p> 	<p>Серверное ПО «Модуль ИБ МИС» (является компонентом МИС), которое определяет права и полномочия пользователей МИС, а также подключаемых дополнительных программно-аппаратных комплексов, рабочих мест администраторов МИС и др.</p>
<p>Сеть удаленной площадки ИС ЛПУ</p> 	<p>ЛВС в границах площадки, на которой располагаются компоненты вычислительной среды</p>
	<p>Каналы связи между ЦОД и удаленными площадками или удаленными пользователями</p>
<p>Шлюз удаленного доступа</p> 	<p>Сервер, который обеспечивает защиту от угроз, связанных с взаимодействием между ЦОД и удаленными площадками или удаленными пользователями по каналам связи, как доверенным, так и каналами общего доступа (Internet)</p>
<p>Сервер ИБ</p> 	<p>Сервер, на котором располагаются компоненты ИБ всей сети</p>
<p>Защита ключами</p> 	<p>Серверное ПО, расположенное на сервере ИБ, которое управляет идентификацией и аутентификацией пользователей и устройств с помощью электронных ключей</p>



<i>Элемент модели мер по защите</i>	<i>Описание элемента</i>
<p>Комплекс средств защиты информации (КСЗИ)</p> 	<p>Серверное ПО, расположенное на сервере ИБ, которое обеспечивает соответствие всей информационной среды техническим мерам, предусмотренным приказом ФСТЭК [5] по защите ПДн</p>
<p>Защита удаленного доступа</p> 	<p>Серверное ПО, расположенное на сервере ИБ, которое регламентирует удаленный доступ в соответствии с установленными политиками ИБ</p>
<p>Рабочее место пользователя с ИС ЛПУ</p> 	<p>Рабочее место пользователя, с которого осуществляется доступ к ИСПДн, входящим в информационную среду</p>
<p>Клиент защиты ключами</p> 	<p>Клиентское ПО, которое входит в состав рабочего места пользователя и обеспечивает идентификацию и аутентификацию, как пользователя, так и программно-аппаратных средств, которые он использует</p>
<p>Клиент КСЗИ</p> 	<p>Клиентское ПО, которое входит в состав рабочего места пользователя и обеспечивает взаимодействие с комплексом средств защиты информации</p>
<p>Клиент удаленного доступа</p> 	<p>Клиентское ПО, которое входит в состав рабочего места пользователя, обеспечивает доступ к удаленным компонентам информационной среды, а также обеспечивает доступ к ресурсам Internet в соответствии с политиками ИБ</p>





ИС МО, обеспечивающий аутентификацию на основе электронных ключей;

- клиента защиты ключами, который обеспечивает взаимодействие рабочего места пользователя ИС МО с сервером защиты ключами.

Системы защиты удаленного доступа состоит из:

- сервера защиты удаленного доступа, который регламентирует удаленный доступ пользователей ИС МО к внешним ресурсам и удаленным площадкам МО;

- клиента удаленного доступа, который обеспечивает взаимодействие рабочего места пользователя ИС МО с сервером защиты удаленного доступа и шлюзом удаленного доступа.

Шлюз удаленного доступа в расширенном варианте решает следующие задачи:

- обеспечение регистрации и доступа в реальном времени к информации о состоянии объектов защищенной сети и текущем значении их сетевых настроек (сервер IP-адресов);

- проксирование защищенного трафика (организация безопасной связи между защищенными сетями через публичные сети);

- оповещение узлов о параметрах доступа друг к другу (сервер IP-адресов);

- организация защищенного взаимодействия с открытым узлом в локальной сети (туннелирование);

- фильтрация открытого и туннелируемого трафика (межсетевой экран);

- выполнение динамической и статической трансляции IP-адресов (NAT);

- организация безопасного подключения компьютеров корпоративной сети к Internet (сервер Открытого Интернета);

- обмен сообщениями/конференция – передача сообщений (с шифрованием) в реальном времени между пользователями сети МО;

- файловый обмен между пользователями сети без установки каких-либо дополнительных служб, например, ftp или совместного использования (sharing) ресурсов;

- вызов внешних приложений – вызов коммуникационных приложений, открытие веб-ссылки и сетевого ресурса общего доступа с автоматической передачей IP-адреса узла защищенной сети;

- проверка соединения с узлом и информирование о статусе пользователя защищенной сети (о би их доступности, активности и т.д.).

В качестве примера рассмотрим один из сценариев, которые возможны при взаимодействии пользователей с МИС МО:

1. Оператор МИС включает на своем рабочем месте персональный компьютер (далее ПК) и дожидается завершения загрузки ОС;

2. Клиент КСЗИ отправляет на сервер КСЗИ данные ПК (MAC-адрес сетевой карты или другие параметры, которые определены политикой ИБ). Если сервер КСЗИ подтверждает правомочность работы ПК в сети, то на экран пользователя выводится приглашение вставить электронный ключ;

3. Оператор МИС вставляет электронный ключ и вводит персональный ПИН-код;

4. Клиент защиты ключами передает введенную информацию на сервер защиты ключами. Если полученные данные корректны, то ПК получает так называемый «билет», в котором прописаны его права и полномочия в системе. В частности, право работать с МИС;

5. Оператор МИС запускает клиентское приложение, которое взаимодействует с МИС. На основании «билета» серверная часть МИС принимает решение о допуске данного пользователя к работе с МИС;

6. Если оператору МИС необходимо обратиться к ресурсам в Internet, то на основании «билета» сервер защиты удаленного доступа разрешает или запрещает данному ПК, за которым работает данный пользователь, обратиться к шлюзу удаленного доступа. Если такое разрешение есть, то информационный поток перенаправляется на шлюз удаленного доступа;

7. Если оператору МИС нужно на некоторое время отлучиться со своего рабочего



места, то он вынимает электронный ключ, что приводит к блокированию ПК. По возвращении, оператор МИС вставляет ключ обратно и вводит ПИН-код. ПК разблокируется;

8. В конце рабочего дня оператор МИС штатно выключает ПК и вынимает электронный ключ.

В процессе работы данного оператора МИС за данным ПК КСЗИ протоколирует все действия, связанные с событиями ИБ, например: время входа в систему, время начала и завершения блокировки, когда выходил в Internet и к какому ресурсу обращался, были ли попытки со стороны внешнего ресурса получить НСД, пытался ли кто-либо во время отсутствия оператора МИС войти на его ПК и др.

Описание внештатных ситуаций, на которые обязан реагировать администратор ИБ МО, выходит за рамки данной статьи, поэтому описание подобных сценариев не приводится.

4. ВЫВОДЫ

Использование МИС налагает на оператора ПДн в лице руководителя МО определенные обязательства перед владельцами

ПДн и законодательством РФ по защите прав владельца ПДн.

Разработка и эксплуатация информационной среды, в частности, компонентов ИБ, которая будет соответствовать всем требованиям законодательства и нормативным актам уполномоченных регуляторов, достаточно трудоемкая задача, решение которой требует высокой квалификации и, как правило, не под силу сотрудникам МО даже, если в составе МО имеется ИТ-подразделение.

Информационная среда, разработанная в соответствии со всеми требованиями законодательства и нормативных документов, может быть аттестована на соответствие этим требованиям организациями, которые уполномочены на проведение аттестации ФСТЭК России и Федеральной службой безопасности Российской Федерации. При этом, в случае возникновения инцидентов, связанных с ИБ, ответственность ложится на разработчика мер по организации ИБ, а также организацию, которая провела аттестацию информационной системы на соответствие требованиям законодательных и нормативных документов.

ЛИТЕРАТУРА



1. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 года № Пр-1895 [Электронный ресурс] / Сайт Совета безопасности Российской Федерации. – Режим доступа: <http://www.scrf.gov.ru/documents/6/5.html>. – Дата доступа: 11.08.2016.
2. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» (с изм. и доп., вступ. в силу с 01.09.2015) [Электронный ресурс] / Официальный сайт компании «Консультант Плюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/. – Дата доступа: 11.08.2016.
3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] / Официальный





- сайт компании «Консультант Плюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/. – Дата доступа: 11.08.2016.
4. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 06.07.2016) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] / Официальный сайт компании «Консультант Плюс». – Режим доступа: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=201168&fld=134&dst=1000000001,0&rnd=0.5916170266366472>. – Дата доступа: 11.08.2016.
 5. Приказ Федеральной службы по техническому и экспортному контролю России от 18.02.2013 г. (зарегистрирован Министерством юстиции РФ 14.05.2013 г.) № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] / Сайт ФСТЭК России. – Режим доступа: <http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21>. – Дата доступа: 11.08.2016.
 6. Федеральный закон от 21 ноября 2011 г. N323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Российская газета. – 23 ноября 2011. – Федеральный выпуск № 5639 (263).
 7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 15.02.2008 г. замдиректора ФСТЭК) [Электронный ресурс] / Сайт ФСТЭК России. – Режим доступа: <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god>. – Дата доступа: 11.08.2016.
 8. Меры защиты информации в государственных информационных системах. Методические указания (утверждены 11.02.2014 г. ФСТЭК России) [Электронный ресурс] / Сайт ФСТЭК России. – Режим доступа: <http://fstec.ru/component/attachments/download/675>. – Дата доступа: 11.08.2016.
 9. Фохт О.А., Цветков А.А. Защита персональных данных. Новое в законодательстве: тенденции, вопросы практического применения в медицинских информационных системах // Научно-практический журнал «Врач и информационные технологии». – 2013. – № 5. – УДК 61:658.011.56.