№ 6 - 2015 г.
14.00.00 медицинские науки
(14.03.00 Медико-биологические науки)

УДК 61+681.3

# ОСОБЕННОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

*Е. Е. Истратова, А. А. Молчанов*

*ГБОУ ВПО «Новосибирский государственный медицинский университет» Минздрава России (г. Новосибирск)*

В статье рассмотрены особенности развития направления по защите персональных данных в медицинских информационных системах. Проанализированы изменения нормативно-правовой базы в отношении защиты персональных данных в учреждениях здравоохранения и требования, предъявляемые к технических средствам защиты информации. Выявлена и обоснована необходимость применения комплексного подхода к вопросу защиты персональных данных, связанная с разработкой защищенных каналов связи между типовой медицинской информационной системой и центром обработки данных.

*Ключевые слова:* защита персональных данных, медицинские информационные системы, защищенные каналы связи.

---

**Истратова Евгения Евгеньевна** — кандидат технических наук, доцент кафедры математики ГБОУ ВПО «Новосибирский государственный медицинский университет», рабочий телефон: 8 (383) 226-55-10, e-mail: istratova@mail.ru

**Молчанов Александр Андреевич** — студент 2-го курса медико-профилактического факультета ГБОУ ВПО «Новосибирский государственный медицинский университет», e-mail: sniper13@211.ru

---

*Введение.*Стремительные темпы развития современных медицинских информационных систем и попытки их интеграции в Единую государственную информационную систему здравоохранения привели к возникновению вопроса о защите персональных данных. Причем разработка данного вопроса ограничивается одновременно двумя факторами — неразвитостью аппаратных и программных средств, применяемых для защиты персональных данных, а также несовершенством нормативно-правовой базы.

*Материалы и методы.* На основе анализа нормативно-правовой документации по защите персональных данных в учреждениях здравоохранения и исследовании основных

требований, предъявляемых к аппаратным и программным средствам по защите персональных данных, выявить основные закономерности и особенности развития направления по защите персональных данных в медицинских информационных системах.

В последнее время в связи с активной разработкой норм и принципов формирования Единой государственной информационной системы здравоохранения возникает вопрос о наиболее эффективных способах объединения различных медицинских учреждений между собой. Данный процесс возможно осуществить при помощи внедрения медицинских информационных систем, являющихся основой формирования региональных и федеральных структурных звеньев. Поскольку этот процесс напрямую затрагивает социальный, медицинский и экономический аспекты жизни населения, то необходимо применение системного подхода, учитывающего как создание отдельных локальных информационных систем, рассчитанных на работу одного лечебно-профилактического учреждения, так и на объединение разрозненных компонентов в единую региональную сеть с выходом на федеральный уровень. При этом ключевой проблемой становится обеспечение защиты персональных данных, используемых в этих медицинских информационных системах.

В общем случае, практически в любой медицинской организации можно выделить два основных подразделения, которые занимаются обработкой информации, связанной с персональными данными. Первое подразделение отвечает за сбор, обработку, хранение, возможную модификацию, уточнение, уничтожение персональных данных пациентов, что связано с проведением непосредственно лечебного процесса, а также формирование медицинской статистической отчетности. Второе подразделение включает в себя такие службы, как отдел кадров и бухгалтерия, и проводит обработку персональных данных сотрудников либо контрагентов.

Помимо этого внутри лечебно-профилактического учреждения может циркулировать менее формализованная информация, содержащая некоторые персональные данные для неограниченного круга лиц. Однако такие данные, как правило, являются обезличенными. В основном к подобным источникам относятся: почтовые клиенты или Интернет-сайты различной направленности.

Причем, если обезличенная информация может передаваться по открытым, т. е. незащищенным сетям связи, то для организации защищенного информационного обмена, осуществляемого в рамках функционирования медицинских информационных систем, необходимым условием является обеспечение криптографической защиты каналов связи, по которым производится передача персональных данных.

При этом на соответствующих объектах информатизации в лечебно-профилактических или любых других медицинских учреждениях, подключаемых к медицинским информационным системам, согласно законодательству, в обязательном порядке должны быть реализованы требования по обеспечению информационной безопасности, регламентируемые текущим законодательством.

*Нормативно-правовая база по защите персональных данных.* Для того, чтобы оценить все особенности защиты персональных данных с точки зрения формирования из отдельных медицинских информационных систем единого государственного информационного портала, необходимо рассмотреть основную законодательную практику, предусмотренную в Российской Федерации с учетом последних изменений.

В качестве основного нормативно-правового документа, регламентирующего защиту персональных данных, можно назвать Федеральный закон № 152 ФЗ «О персональных

данных» от 27.07.2006 с учетом всех принятых позднее изменений и дополнений. В этом законе не только дается понятие о персональных данных, но и регулируются возможные, в том числе в медицинском учреждении, отношения по сбору, обработке и хранению информации, связанной с субъектами персональных данных [1].

Согласно данному закону, к персональным данным относится любая информация о физическом лице: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, идентификационные данные документов (паспорт, СНИЛС и т. п.), семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация. При этом под обработкой персональных данных понимаются такие действия с ними, как систематизация, накопление, хранение, уточнение, использование, распространение, обезличивание, блокирование, а также уничтожение данных.

Еще одним нормативно-правовым актом, определяющим использование персональных данных, является Постановление Правительства Российской Федерации № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008. Согласно этому документу, обработка персональных данных, содержащихся в защищенной системе либо извлеченных из подобной системы, считается неавтоматизированной, если такие действия с этими данными, как использование, уточнение, распространение и уничтожение относительно каждого из субъектов персональных данных осуществляются при непосредственном участии самого субъекта, т. е. человека [2].

Однако данный документ имеет некоторые ограничения. Так, обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только потому, что персональные данные содержатся в информационной системе либо были извлечены из нее. При этом в самом положении четко определяются правила и основные требования, предъявляемые к обработке персональных данных, осуществляемой без использования средств автоматизации.

В более позднем Постановлении Правительства Российской Федерации от 1 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» № 1119 уже строго прописываются требования, направленные на обеспечение информационной безопасности. Согласно этому Постановлению, защищенная система представляет собой информационную среду, обрабатывающую специальные категории персональных данных, в том числе, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных [3].

В тексте положения устанавливаются требования к обеспечению безопасности персональных данных при их обработке в защищенной сети с помощью систем защиты персональных данных, среди которых можно выделить следующие группы мероприятий:

- организационные меры;
- средства защиты информации (в том числе и шифровальные средства);
- средства предотвращения несанкционированного доступа;
- средства предотвращения утечки информации по техническим каналам;
- программно-технические воздействия на технические средства обработки персональных данных.

В определенном смысле переломным моментом в развитии нормативно-правовой базы по защите персональных данных можно считать Приказ Федеральной службы

безопасности Российской Федерации № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2013. Благодаря появлению данного документа, была реализована первая попытка объединения в одном нормативно-правовом акте самых основных моментов, связанных с защитой персональных данных. Помимо этого, в данном документе приводится предварительная классификация всех средств и систем защиты информации, имеющей непосредственное отношение к персональным данным [4].

В последующих приказах Федеральной службы безопасности Российской Федерации, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации № 55/86/20 от 13.02.2008 устанавливается баланс, необходимый для продолжения внедрения осмысленной классификации медицинских информационных систем [5].

Анализ рассмотренной законодательной базы показывает, что в качестве основных мер, обеспечивающих поддержание стабильно надежного уровня защиты передаваемых в региональный или федеральный центр обработки персональных данных, необходимо применять защищенные каналы связи. Также нельзя не отметить попытки законодательного формирования принципов и критериев классификации медицинских информационных систем.

*Защищенные каналы связи для передачи персональных данных.* Помимо законодательной составляющей, регламентирующей те или иные правила и принципы организации и внедрения защищенных каналов связи для передачи данных, необходимо также исследовать конкретные технологии, позволяющие претворять в жизнь данные идеи.

Согласно Методическим рекомендациям медицинским организациям по разработке криптографической защиты каналов, при взаимодействии в рамках создания единого информационного портала, для организации криптографической защиты каналов связи при информационном обмене в составе медицинских информационных систем используются технологии построения виртуальных частных сетей.

При этом под подобной виртуальной частной сетью (от английского Virtual Private Network, то есть VPN) понимается общее название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Даже, несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям. Осуществляется это, благодаря применению средств криптографии (шифрования, аутентификации, технологии открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

Таким образом, современные средства построения VPN, помимо организации собственно виртуальной сети, также позволяют выполнить требования защиты данных при их сетевом обмене. При этом большинство современных VPN-решений используют технологии инкапсуляции для создания инфраструктуры виртуальной сети и средства шифрования данных для их защиты в процессе передачи.

В качестве основных требований, предъявляемых к тем или иным информационным продуктам, разработанным на основе VPN-технологии относятся:

1. Обеспечение безопасности персональных данных. Так как уровень безопасности

является одним из наиболее важных критериев в процессе защиты персональных данных, то, очевидно, что конкретное VPN-решение должно удовлетворять данному требованию. Однако при этом не стоит забывать, что процесс обеспечения безопасности представляет собой комплексную задачу, т. е. применение VPN-технологии должно осуществляться в сочетании с firewall-защитой и интегрированными дополнительными приложениями безопасности, например такими, как мониторинг вторжений, поддержка цифровых сертификатов, Radius-функции и идентификация клиентов. Только в данном случае VPN-решение позволит создать единую достаточно мощную коммуникационную платформу, которая позволит передавать персональные данные от отдельной медицинской информационной к региональному центру обработки данных.

2. Гибкость и надежность соединения, связанные с тем, что оборудование для VPN-инфраструктуры должно поддерживать разнообразные архитектуры и протоколы, т. е. VPN-системы должны иметь много сетевых интерфейсов, поддерживать совместимость с существующим оборудованием, устраняя потребность в установке дополнительных сетевых устройств. Помимо этого, VPN-решение также должно включать в себя надежные функции зашиты от сбоев практически для всех аппаратных и программных компонентов, как и в любой другой сетевой инфраструктуре. Конфигурации портов должны включать в себя поддержку на случай сбоев, чтобы при отказе порта задачу можно было автоматически перевести на другой порт, что, в свою очередь, позволит поддерживать высокую работоспособность сети.

3. Легкость управления. Управление не случайно является важным критерием при выборе того или иного VPN-решения, так как продвинутые функции сетевого управления уменьшают необходимость использования дополнительного оборудования, а также предлагают детальные функции отчетности и оповещения о выявленных инцидентах. Таким образом, полноценное VPN-решение для целей управления должно предоставлять сетевым администраторам простые инструменты интегрированного доступа удаленного и локального управления. Единая точка контроля также необходима для мониторинга посредством поддержки широко распространенных инструментов управления корпоративного класса.

Развитие VPN-продуктов привело к тому, что теперь они могут интегрировать множество VPN-требований в одной системе, включая firewall, балансировку нагрузок, проверку URL, отслеживание вторжений и инициализации отказа в обслуживании, антивирусную защиту, маршрутизацию и управление. Централизация ключевых функций является важнейшим звеном для управления критическими VPN-приложениями, поддерживающими цифровые ресурсы медицинской организации.

Таким образом, анализ требований к VPN-технологиям, используемым в медицине, показал, что наиболее приемлемыми программными и программно-аппаратными комплексами является информационный продукт VIPNet, предоставляющий широкий спектр возможностей для построения виртуальных сетей от объединения в единую сеть нескольких компьютеров до создания глобальных распределенных виртуальных сетей, совокупно объединяющих десятки тысяч узлов, для медицинских учреждений с большим числом территориально удаленных подразделений.

*Выводы*

1. Анализ нормативно-правовой базы о защите персональных данных показал две основные тенденции. Первая из них связана с попытками классифицировать существующие медицинские информационные системы с целью выявления

их положительных и рациональных особенностей для последующего создания на их основе универсального шаблона для разработки новых медицинских информационных систем. Вторая тенденция связана с проработкой законодательной базы в области разработки, внедрения, сопровождения и других организационных моментов, связанных с созданием защищенных каналов связи, по которым предполагается передача персональных данных между медицинскими информационными системами и региональными центрами обработки данных.

2. Выявление особенностей развития законодательной базы, посвященной вопросу защиты персональных данных в медицинских информационных системах при их интеграции в единое информационное медицинское пространство невозможно рассматривать отдельно от изучения существующей аппаратной и программной составляющих, обеспечивающих реализацию данного процесса.

*Список литературы*


1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. От 04.06.2014) «О персональных данных».
2. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. Приказ ФСБ РФ от 14.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. Приказ ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13.02.2008 «Об утверждении Порядка проведения классификации информационных систем персональных данных» (Зарегистрировано в Минюсте РФ 03.04.2008 № 11462).

# FEATURES OF PROTECTION OF PERSONAL INFORMATION IN MEDICAL INFORMATION SYSTEMS

*E. E. Istratova, A. A. Molchanov*

*SBEI HPE «Novosibirsk State Medical University of Ministry of Health» (Novosibirsk)*

Features of development of the direction in protection of personal information in medical information systems are considered in the article. Changes of standard and legal base concerning protection of personal information in healthcare institutions and requirements imposed to technical to information means of protection are analysed. The necessity of application of an integrated approach to a question of protection of personal information connected with development of the protected communication channels between sample medical information system and a data-processing center is revealed and proved.

***Keywords**:* protection of personal information, medical information systems, the protected communication channels.

---

**About authors:**

**Istratova Evgenia Evgenyevna** — candidate of technical science, assistant professor of mathematics chair at SBEI HPE «Novosibirsk State Medical University of Ministry of Health», office phone: 8 (383) 226-55-10, e-mail: istratova@mail.ru

**Molchanov Alexander Andreevich** — student of the 2nd course of medico-preventive faculty at SBEI HPE «Novosibirsk State Medical University of Ministry of Health», e-mail: sniper13@211.ru

**List of the Literature:**

1. Federal law of 27.07.2006 N 152-FZ (edition. Of 04.06.2014) «About personal information».
2. The resolution of the Government of the Russian Federation of 15.09.2008 N 687 «About the adoption of Provision on features of the processing of personal information which is carried out without usage of an automation equipment».
3. The resolution of the Government of the Russian Federation of 01.11.2012 N 1119 «About the approval of demands to protection of personal information at their processing in information systems of personal information».
4. The order of FSC of the Russian Federation of 14.02.2013 N 21 «About the statement of Structure and the maintenance of organizational and technical measures for safety of personal information at their processing in information systems of personal information».
5. The order FSTEC of the Russian Federation N 55, FSC of the Russian Federation N 86, the Ministry of Information Technologies and Communications of the Russian Federation N 20 of 13.02.2008 «About the statement of the Order of carrying out classification of information systems of personal information» (03.04.2008 N 11462 registered in Ministry of Justice of the Russian Federation).