



Код безопасности
ГК «Информзащита»

Особенности защиты персональных данных в медицинской отрасли

М. Ю. Емельяников, директор по развитию бизнеса ЗАО НИП «Информзащита»

Введение

Как известно, у медали – всегда две стороны. И оборотная сторона может совсем не радовать обладателя. Так и новейшие технологии, даря невиданные ранее возможности, всегда несут и новые риски, и новые угрозы.

В полной мере справедливость этих банальных истин (а банальности справедливы всегда – именно потому они таковыми и становятся) почувствовали на себе все без исключения предприятия и организации, с энтузиазмом переключившие последние лет двадцать на мощные компьютерные плечи проблемы учета кадров, расчета заработной платы, взаимоотношений с заказчиками, клиентами, абонентами и пациентами. Правительством поставлена задача перевода к 2015 году всех медицинских учреждений на электронные медицинские карты, удаленную запись к врачам и создания единого регистра медицинского персонала.

Но грянул гром, которого поначалу никто не услышал. Еще в декабре 2005 г. Россия ратифицировала Европейскую конвенцию о защите физических лиц при автоматизированной обработке персональных данных и в июле 2006 г. приняла, в соответствии с взятыми при ратификации обязательствами, Федеральный закон «О персональных данных» (далее – ФЗ-152). Все обладатели компьютеров и программ для них, в которых в качестве данных для обработки использовались фамилии, имена и отчества физических лиц, в одночасье получили загадочное звание «операторов персональных данных», а информационные сети и отдельные компьютеры превратились в информационные системы персональных данных (ИСПДн). Государство назначило органы, осущест-

вляющие контроль и надзор за выполнением этих самых требований, – Роскомнадзор (выполнение закона в целом), ФСБ России (применение криптографических средств защиты) и ФСТЭК России (использование всех остальных средств информационной безопасности). В течение небольшого промежутка времени появились требования по защите этих самых персональных данных и информационных систем (три постановления Правительства РФ), обязательные для выполнения всеми без исключения операторами.

За четыре года провозмещения выяснилось, что закон порождает массу почти неразрешимых проблем, содержит невыполнимые нормы, не обеспечивает баланса интересов личности, государства и этих самых операторов и в таком виде может быть и не нужен. Недаром срок приведения информационных систем персональных данных в соответствие установленным требованиям в конце прошлого года спешно был перенесен на год, а 7 декабря уже этого года в первом чтении Думой приняты поправки, отодвигающие сроки окончания работ еще на один год.

Но, как завещали мудрые римляне, “Dura lex, sed lex” – «Закон суров, но это закон». И пока он существует в нынешнем виде, выполнять надо именно его. И надзирать будут перечисленные органы именно за его выполнением.

Между тем реализация требований закона – проблема непростая, а специфика деятельности медицинских учреждений привносит в работу по наведению порядка в обработке персональных данных свою, весьма существенную, специфику.

Специфика обработки персональных данных в медицинских учреждениях

Больницы, поликлиники, госпитали, амбулатории и прочие лечебные учреждения как операторы персональных данных получили дополнительные ограничения и требования, которых нет у большинства иных операторов.

Сведения о состоянии здоровья и интимной жизни были отнесены законом к специальным категориям персональных данных. Обрабатывать их можно только при наличии письменного согласия пациента – субъекта персональных данных. Исключений из этого правила всего два:

- когда обработка сведений о состоянии здоровья необходима для защиты жизни, здоровья или иных

жизненно важных интересов субъекта либо жизни, здоровья или иных жизненно важных интересов других лиц, а получение согласия субъекта персональных данных невозможно;

- когда обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным, в соответствии с законодательством Российской Федерации, сохранять врачебную тайну (т.е. непосредственно врачом).

Подобные ограничения создают существенные проблемы для медицинских учреждений – даже на то, чтобы сведения в электронную историю болезней или электронную амбулаторную карту вносила медсестра, ассистирующая врачу при приеме или лечении, нужно письменное (!) согласие пациента. Возникает проблема с доступом к информации подразделений автоматизации, государственных и муниципальных служащих департаментов и отделов здравоохранения органов власти, не являющихся врачами, в том числе – при подготовке и обработке многочисленных отчетов, содержащих необезличенные данные о больных и их лечении.

Такой порядок делает практически невозможным хостинг приложений медицинских учреждений в центрах обработки данных (ЦОД), использование передовых технологий, например, облачных и вычислений SaaS, поскольку в этом случае определить лиц, имеющих доступ к персональным данным, практически невозможно.

Дело в том, что согласие пациента на обработку должно содержать, в том числе, цель обработки персональных данных, перечень персональных данных, на обработку которых дается согласие, перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных. Как вытекает из приведенного выше ограничения на доступ лиц, не являющихся врачами, к персональным данным пациентов, в согласии на обработку придется указать и тех лиц, которые будут допущены к сведениям о состоянии здоровья. Предусмотреть все это заранее весьма сложно, а невыполнение требований к содержанию согласия на обработку приведет к санкциям надзирающих органов, как это произошло, по информации, размещенной на сайте Роскомнадзора, при проверке его территориальными подразделениями Центральной районной больницы Морозовского района Ростовской области и Городской больницы №1 г. Азова.

Вторая специфическая проблема обработки персональных данных пациентов, содержащих сведения о состоянии здоровья, вытекает из первой.

Правительство РФ Постановлением 2007 г. №781 утвердило «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», в котором содержится требование об обязательной классификации всех ИСПДн. Классификацию проводят сами операторы (в нашем случае – медицинские учреждения), а порядок ее определяется трехсторонним приказом ФСТЭК России, ФСБ России и Мининформсвязи от 13 февраля 2008 г. №55/86/20. В соответствии с этим приказом информационные системы, обрабатывающие сведения о состоянии здоровья, отнесены одновременно к типовым системам класса К1 и специальным системам. Такое сочетание означает, что если в ходе обработки персональных данных будут нарушены заданные характеристики безопасности персональных данных, последствия такого нарушения для субъектов персональных данных априори оцениваются как значительные негативные. С целью выявления актуальных угроз персональным данным в таких системах необходимо формирование модели угроз в соответствии с методиками ФСТЭК России, а при применении криптографических средств защиты – и ФСБ России.

Отнесение ИСПДн медицинских учреждений к наиболее высокому из всех возможных классов требует принятия наиболее полных и, соответственно, сложных способов и методов защиты информации, включая обязательную сертификацию всех средств защиты не только по функциональным требованиям, но и подтверждающую отсутствие у них недекларированных возможностей – т. е. функциональных возможностей, не описанных или не соответствующих описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. А выбор таких средств не так уж и велик, и подавляющее большинство из них – отечественного производства, поскольку сертификация на отсутствие недекларированных возможностей требует раскрытия исходных кодов, на что зарубежные вендоры идут крайне неохотно.

Как привести порядок обработки данных в ИСПДн в соответствие закону

Как мы уже отмечали, наличие специфики работы с персональными данными вовсе не отменяет обязательности выполнения установленных требований.

Сразу необходимо отметить, что создание подсистемы безопасности ИСПДн подпадает под категорию мероприятий по технической защите конфиденциальной информации, а этот вид деятельности является лицензируемым, и проведение таких работ даже для собственных нужд без соответствующей лицензии является нарушением закона. Обязательному лицензированию подлежит также деятельность по техническому обслуживанию и распространению шифровальных средств, под которую подпадает, например, приобретение и установка в удаленных филиалах или структурных подразделениях медицинского учреждения или органа здравоохранения криптографических средств защиты информации.

Лицензионные требования для указанных видов деятельности довольно сложны и чаще всего неподъемны для медицинского учреждения. Перечислять их не будем, отметим лишь, что получение лицензии предусматривает, например, наличие в штате не менее двух специалистов, имеющих профильное образование по защите информации или государственные документы о повышении квалификации в данной области.

В случае отсутствия лицензий у медицинского учреждения или органа здравоохранения, для проведения соответствующих проектных и пусконаладочных работ необходимо привлечение специализированной организации, имеющей такие лицензии (или лицензию).

Первым шагом в наведении «законного порядка» должна стать инвентаризация всех информационных систем медучреждения и выявление среди них тех, которые подпадают под определение ИСПДн. Помимо приложений, обрабатывающих сведения о пациентах, к ним, безусловно, относятся системы удаленной записи на прием к врачу, системы кадрового и бухгалтерского учета самого учреждения, системы электронной почты, справочные порталы и даже системы управления идентификацией и доступом, если в них содержатся персональные данные пользователей информационной системы.

Для каждой такой ИСПДн необходимо создать модель угроз персональным данным, исходя из условий ее функционирования. Модель угроз и параметры ИСПДн, такие как категория персональных данных (т. е. собственно их содержание) и количество субъектов, чьи данные обрабатываются в системе,

определяют класс ИСПДн. Результаты классификации документируются (отражаются в актах). Вид ИСПДн (типовая или специальная) и ее класс будут определяющими при выборе способов и методов защиты персональных данных, поэтому ни в коем случае к этой работе нельзя подходить формально – затраты на обеспечение безопасности могут оказаться абсолютно неприемлемыми. В ходе аналитической работы по формированию модели угроз и определению класса ИСПДн необходимо исходить не из текущей, а из планируемой топологии информационной системы.

Поясню на примере. Как уже отмечалось, ИСПДн, содержащие сведения о состоянии здоровья, относятся к специальным класса К1. Но, после реинжиниринга, класс систем вполне можно изменить. Наиболее радикальным способом является обезличивание персональных данных в системе, обрабатывающей данные пациентов. Если ИСПДн поликлиники разделить на две системы – базу данных с электронными медицинскими картами, в которой данные обезличены и вместо фамилии, имени и отчества пациентов используются некие условные коды (например, номера полисов обязательного медицинского страхования или любые другие) и базу данных пациентов, где нет сведений о состоянии здоровья, а есть только связь между условным кодом истории болезней и идентифицирующими пациента данными, то вместо одной большой системы получим две. Первая, обезличенная, является специальной системой класса К4 и не требует обеспечения конфиденциальности данных. Вторая, в которой медицинских данных нет, – типовая система класса К3. Затраты на выполнение обязательных требований по защите информации для специальной системы класса К1 и двух систем класса К3 и К4 несопоставимы и отличаются на два, и иногда на три порядка. Система К4, грубо говоря, требует только обеспечения целостности и доступности информации, для чего вполне достаточно системы резервного копирования, без которой ни один уважающий себя ИТ-директор не обойдется в любом случае, даже и без требований к ИСПДн, а сертифицированные средства защиты информации (СЗИ) для нее вообще не нужны. Система К3 может быть размещена на локальном компьютере регистратуры, на который, скорее всего, будет достаточно установить средство защиты от несанкционированного доступа (НСД), например Secret Net, и программу антивирусной защиты. Затраты не превысят 10 тысяч рублей. В специальной системе класса К1, да еще подключенной к Интернету, без чего современное лечебное учреждение вряд ли

обойдется, будут необходимы сертифицированные системы межсетевое экранирования, обнаружения и предупреждения вторжений, антивирусной защиты (на всех узлах), предотвращения НСД (на всех серверах и рабочих станциях), сканеры безопасности – как минимум. Не следует забывать про сертификацию по требованиям отсутствия недекларированных возможностей (НДВ). Несколько миллионов рублей затрат гарантированы.

Мне приходилось не раз сталкиваться со скептическими мнениями об эффективности и целесообразности обезличивания ИСПДн в медицине. Аргументы скептиков не впечатляют и не убеждают.

Когда класс системы и модель угроз определены, пора приступать к построению подсистемы безопасности ИСПДн. Алгоритм здесь простой. Для каждой актуальной угрозы необходимо определить способы ее нейтрализации (снижения до приемлемого уровня), выбрать механизмы защиты, нейтрализующие эту угрозу, определить, исходя из класса системы и возможностей нарушителя, конкретные функциональные требования к таким механизмам защиты, и наконец-то выбрать средства защиты, соответствующие этим функциональным требованиям. Для этого необходимо использовать «инструментальные ящики», содержащие описание всех необходимых средств, – Положение о методах и способах защиты информации в ИСПДн (Приказ ФСТЭК России от 05.02.2010 г. №58) и Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в ИСПДн с использованием средств автоматизации (утверждены руководством 8 Центра ФСБ России 21.02.2008 г. №149/54-144).

Выполнение этих работ потребует глубокого знания архитектуры информационных систем, характеристик и возможностей общего (операционные системы) и прикладного (приложения) программного обеспечения, продуктовой линейки средств защиты различных производителей и многого другого, но ведь для этого и существуют специалисты в специализированных организациях!

Чтобы не создавать «зоопарк» систем защиты, так нелюбимого всеми ИТ-специалистами и попортившего немало их крови из-за сложности интеграции и обслуживания, целесообразно искать производителя СЗИ, имеющего максимально длинную линейку продуктов, легко интегрируемых в единую систему безопасности. Таким путем идет компания «Код Безопасности», последовательно наращивающая функциональные возможности своих продуктов и имеющая на сегодняшний день в своем арсенале средства предотвращения НСД (в том числе – и

в виртуальной среде), доверенной загрузки, шифрования, межсетевое экранирование (в том числе – персональные межсетевые экраны для рабочих станций), защиты от вторжений и антивирусной защиты (http://www.securitycode.ru/solutions/security_studio/). Все они сертифицированы, большинство – под максимальный класс ИСПДн К1, многие – и по требованиям отсутствия НДВ.

Результаты проектной работы оформляются документально, поскольку упомянутое выше «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» требует обязательного наличия описания ИСПДн.

Документируются и результаты пусконаладочных работ по установке и введению в эксплуатацию средств защиты информации, поскольку тем же положением предусматривается составление заключений о возможности эксплуатации СЗИ.

Не надо забывать об обучении персонала, эксплуатирующего средства безопасности, поскольку это тоже обязательное требование к системе защиты.

Система защиты создана, запущена в промышленную эксплуатацию – наступило время почитать на лаврах? Как бы не так. Необходимо запустить эффективную систему мониторинга уровня защищенности и работы средств защиты, обеспечивающую возможность выявления фактов несоблюдения условий использования СЗИ, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защиты, возможность проведения расследований и составления заключений по фактам нарушений, а также формирование заключений по их результатам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений впредь.

А здесь трудно обойтись без сканеров и мониторов защищенности, систем управления событиями информационной безопасности и инцидентами, систем корреляции событий, обычно обозначаемых аббревиатурой SIEM (Security Information and Event Management).

Несколько слов о проблемах, не решаемых рассматриваемыми нормативными документами. Причем проблемы здесь не технические, с ними все более-менее понятно, а правовые. Очень трудно добиться легитимности применения веб-форм для обработки персональных данных, без которого современные приложения в медицинских учреждениях немислимы – их используют электронные больницы и поликлиники, системы самозаписи на прием к врачу и вызова

врача на дом, системы телемедицины и облачного хранения медицинской информации. Проблема состоит в необходимости доказывания того, что веб-форма заполняется самим субъектом, а не кем-то от его имени. Без ЭЦП или предварительной раздачи логинов-паролей или идентификаторов здесь обойтись трудно, а необходимость их использования сводит на нет большинство преимуществ веб-технологий.

Вторая проблема – в требовании закона об уничтожении персональных данных в трехдневный срок после достижения цели их обработки или по требованию субъекта. Такой подход полностью противоречит самой сути ведения истории болезни, амбулатор-

ных и медицинских карт, логике построения системы здравоохранения и профилактики болезней.

Есть ряд проблем, не полностью связанных с техническими вопросами, но весьма болезненных для медицинских учреждений. Это, например, возможность получения данных о пациенте не от него, а от третьих лиц (в том числе по средствам связи и сетевого обмена) – при записи больного на прием, вызове врача, медицинском страховании или размещении информации о врачах на сайтах в сети Интернет, требующее получения письменного и весьма пространного согласия на это каждого конкретного врача.

Несколько слов в заключение

Эффективное решение проблем, связанных с выполнением законодательных требований по обработке персональных данных, в первую очередь – обеспечение их безопасности с учетом специфики деятельности медицинских учреждений – требует глубокой методической проработки вопросов, трансляции требований, рассчитанных на профессионалов в области информационной безопасности на язык, понятный руководителям лечебных организаций и персоналу подразделений автоматизации. Работа, проводимая в этом направлении Минздравсоцразвития, очень важна, но, как представляется, еще недостаточна. Разработанные по заказу министерства методические материалы не дают ответов на наиболее сложные, острые вопросы, возникающие при реализации положений нормативно-правовых актов, особенно в медицинских учреждениях с современной инфраструктурой, использующих наиболее передовые технологии, современное компьютеризированное медицинское и лабораторное оборудование, интегрированное с информационными системами.

Выход видится в кооперации усилий профессионалов в области медицинских информационных техно-

логий, как создающих, так и эксплуатирующих прикладные системы, а также специалистов в области информационной безопасности, имеющих необходимые специальные знания. Их совместными усилиями были бы возможны создание глубоких, учитывающих все особенности работы медицинских информационных систем отраслевых нормативных и методических документов, апробация в реальных условиях деятельности организаций системы здравоохранения и согласование документов с государственными регуляторами.

Тогда медицинские учреждения занимались бы своей основной работой – лечили людей, а не решали сложные кроссворды российского законодательства, имели бы возможность использовать самые современные достижения медицины, не опасаясь невольно стать правонарушителями. Это позволило бы и сформулировать требования безопасности к медицинским прикладным системам, и заняться их реализацией уже на этапе создания программного обеспечения, а не решать задачу «прикручивания» средств безопасности на этапе их ввода в эксплуатацию.



Код безопасности

ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.

Адрес офиса в Москве: ул. Образцова, д. 38.

Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.

Тел.: +7 (495) 980-2345 (многоканальный).

Факс: +7 (495) 980-2345.

E-mail: info@securitycode.ru

Запрос дополнительной информации о продуктах: info@securitycode.ru

По вопросам стоимости и покупки продуктов sales@securitycode.ru

По вопросам партнерства и сотрудничества info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте

www.securitycode.ru

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.