Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ПРОБЛЕМА ОБЕЗЛИЧИВАНИЯ ДАННЫХ ПРИ СОЗДАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ В ОБЛАСТИ ЗДРАВООХРАНЕНИЯ

А.Б. СТЕПАНЯН, В.А. ДМИТРИЕВ, Е.П. МАКСИМОВИЧ, В.К. ФИСЕНКО

Объединенный институт проблем информатики НАН Беларуси

В настоящее время в Республике Беларусь наблюдается интенсивное внедрение информационных технологий в медицину. Успешное развитие данного направления невозможно без создания соответствующего нормативно-методологического базиса, аккумулирующего как, накопленный опыт развития современных информационных технологий, так и специфику предметной области. В международной практике уже действуют стандарты ISO и аналогичные российские стандарты в области информатизации здоровья (Health informatics). В РБ также начались подобные работы – в области информатизации здоровья действуют либо подлежат введению в текущем году шесть ГОСТ-межгосударственных стандартов. При этом стандарты ГОСТ ISO/TS 22600-3, касающийся управления привилегиями и контроля доступа в медицинских информационных системах, связан с вопросами информационной безопасности. В то же время, как показала практика создания реальных информационных систем, существующие НПА и ТНПА РБ не охватывают ряд важных аспектов защиты медицинской информации и тем самым не обеспечивают необходимую нормативно-техническую базу, позволяющую учесть все важные уязвимости безопасности и выработать совокупность требований безопасности, обеспечивающих полное решение возникающих проблем безопасности.

Одной из ключевых проблем защиты медицинской информации является обеспечение конфиденциальности идентификационных данных пациента, определяющих его личность. С юридической точки зрения и защиты прав человека персональная медицинская информация имеет большую степень чувствительности и требует применения соответствующих мер защиты. С этой целью принято Постановление Министерства здравоохранения Республики Беларусь от 01.07.2002 № 46 «Об утверждении Положения о порядке и условиях оказания медицинской помощи анонимно».

Для повышения ответственности медицинского персонала или иных работников, связанных с обработкой медицинской информации, предусмотрена статья 178 Уголовного кодекса Республики Беларусь, которая гласит: «1. Умышленное разглашение медицинским, фармацевтическим или иным работником без профессиональной или служебной необходимости сведений о заболевании или результатах медицинского освидетельствования пациента (разглашение врачебной тайны) – наказывается штрафом или лишением права занимать определенные должности или заниматься определенной деятельностью. 2. Разглашение врачебной тайны, выразившееся в сообщении сведений о наличии у лица ВИЧ-инфекции или заболевания СПИД, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет. 3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие тяжкие последствия, – наказываются лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения».

Для решения проблемы обеспечения конфиденциальности персональных медицинских данных в медицинских информационных системах используется обезличивание данных. Однако механизм обезличивания данных не затрагивается ни одним НПА

и ТНПА Республики Беларусь, что затрудняет его практическую реализацию при создании реальных информационных систем.

Особо остро проблема конфиденциальности персональных медицинских данных проявилась в ходе создания системы защиты информации автоматизированной информационной системы сбора и анализа данных Республиканского регистра ВИЧ-инфицированных пациентов (далее АИС ВИЧ). АИС ВИЧ предназначена для применения в профильных подразделениях на объектах учреждений здравоохранения в целях централизованного мониторинга больных с ВИЧ, автоматизации процессов учета случаев заболевания, централизованной обработки информации о больных с ВИЧ, их клиническом сопровождении, проводимой антиретровирусной терапии, а также позволяет обеспечить Министерство здравоохранения РБ эффективным средством информационной поддержки при принятии управленческих решений по контролю ВИЧ. Основными видами автоматизируемой деятельности в АИС ВИЧ являются ведение единого республиканского регистра ВИЧ и выдача информации из регистра полномочным организациям и должностным лицам, осуществляющим диспансерное наблюдение за пациентами и эпидемиологическое наблюдение и статистический учет случаев ВИЧ инфекции. Ведение регистра осуществляется посредством сбора, накопления, своевременной актуализации, обработки, архивирования и резервного копирования данных. Ключевыми аспектами ведения регистра ВИЧ являются обеспечение достоверности, конфиденциальности, целостности и доступности данных, хранящихся в регистре и передаваемых из территориальных профильных подразделений учреждений здравоохранения.

Регистр ВИЧ функционирует на четырех уровнях:

– первый уровень – лаборатории, осуществляющие диагностику ВИЧ/СПИД, создающие бумажное и (или) электронное сообщение о положительном результате исследования в подтверждающем тесте на ВИЧ-инфекцию и передачу информации на областной (Минский городской) уровень регистра с целью добавления в регистр подтвержденных случаев ВИЧ-инфекции;

– второй уровень (районный) – районные санитарно-эпидемиологические учреждения, осуществляющие эпидемиологическое наблюдение и статистический учет случаев ВИЧ инфекции, а также организации здравоохранения районного уровня, осуществляющие диспансерное наблюдение за пациентами. Уполномоченные должностные лица этого и следующего уровней осуществляют (по внешним каналам связи) формирование, актуализацию и использование данных регистра о наблюдаемых пациентах;

– третий уровень (областной, Минский городской) – областные (Минский городской) санитарно-эпидемиологические учреждения, осуществляющие эпидемиологическое наблюдение и статистический учет случаев ВИЧ-инфекции, а также организации здравоохранения областного (Минского городского) уровня, осуществляющие диспансерное наблюдение за пациентами;

– четвертый уровень (республиканский) – Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения, Республиканский центр гигиены, эпидемиологии и общественного здоровья и Министерство здравоохранения РБ. На этом уровне осуществляется управление регистром, организационная поддержка его функционирования, разработка нормативных, методических документов, информационно-справочных материалов и др.

Анализ уязвимостей (угроз) безопасности показал, что в системе защиты информации АИС ВИЧ необходимо помимо стандартных технических мер защиты информации (идентификация и аутентификация, управление доступом, регистрация событий безопасности, управление безопасностью, антивирусная защита, межсетевое экранирование, обнаружение/предотвращение вторжений, защищенная передача данных

по внешним каналам связи с использованием криптографических средств) использовать также обезличивание данных. Однако эта мера не упоминается в НПА и ТНПА РБ по защите информации. Это затрудняет применение обезличивания данных, хотя в случае АИС ВИЧ оно приобретает особую актуальность в виду социально-экономической и медицинской значимости информации о наличии у физического лица ВИЧ.

В соответствии с международным стандартом ИСО/ТС 25237 [1] и его российским аналогом ГОСТ Р 55036 [2] сокрытие личности ВИЧ-инфицированного пациента осуществляется путем замены его идентификационных данных специально сформированными псевдонимами.

В соответствии с критериями идентификации персональные данные можно разделить на две части: обрабатываемые обезличенные данные (часть данных, содержащая характеристики, по которым субъект данных не может быть однозначно идентифицирован) и идентифицирующие данные (часть данных, содержащая совокупность характеристик, по которым субъект данных может быть однозначно идентифицирован).

Обезличивание представляет собой процесс удаления связи между идентифицирующей совокупностью характеристик и субъектом данных. Оно может быть осуществлено двумя разными способами: а) с помощью удаления или преобразования характеристик, когда связь между характеристиками и субъектом данных либо разрывается, либо перестает быть уникальной и указывает на несколько субъектов данных; б) путем увеличения популяции субъектов данных, при котором связь между совокупностью характеристик и субъектом данных перестает быть уникальной.

Псевдонимизация – особый случай обезличивания, при котором помимо удаления прямой связи с субъектом данных создается связь между конкретной совокупностью характеристик этого субъекта и одним или несколькими псевдонимами. Поскольку существуют связи между совокупностями характеристик и псевдонимами, то с функциональной точки зрения между несколькими псевдонимизированными совокупностями данных, относящимся к одному и тому же субъекту, можно установить связь, не раскрывая его идентичность. Псевдонимизация может быть обратимой или необратимой, то есть может позволять или не позволять восстановление идентичности субъекта данных. При обратимой псевдонимизации должен быть определен способ восстановления связи между совокупностью характеристик и субъектом данных. Для АИС ВИЧ актуальна обратимая псевдонимизация.

Организация применения псевдонимов в здравоохранении, когда вся информация должна быть документирована и юридически значима, требует соответствующего правового обеспечения. В соответствии с существующей международной практикой целесообразно создать специальную службу псевдонимизации, организующую работу с псевдонимами пациентов и удаленный доступ лечащих врачей с использованием псевдонимов. Службу псевдонимизации является автономным компонентом, основное назначение которого – генерация уникальных идентификаторов.

Таким образом, как показывает практика, для обеспечения информационной безопасности создаваемых медицинских информационных системах в РБ актуально принятие ТНПА, регламентирующего механизм псевдонимизации с учетом существующих международных стандартов [1,2].

Список литературы

1. ISO/TS 25237:2008 "Health informatics - Pseudonymization"

2. ГОСТ Р 55036-2012 ISO/TS 25237:2008. «Информатизация здоровья. Псевдонимизация».