УДК 004.056.5

ОСНОВНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Е.А. МЕНИЦКИЙ
(Представлено: канд. физ.-мат. наук., доц. Д.Ф. ПАСТУХОВ)

В статье представлены основные аспекты архитектурных особенностей по предоставлению безопасности и защищенности конфиденциальных данных в медицинских информационных системах. Рассмотрен алгоритм работы технологии распределения прав доступа к медицинской информации.

Ключевые слова: *информационные технологии, медицинская информационная система, шифрование данных, защищенность данных.*

Введение. С увеличением объема концентрируемой информации в сфере медицины, возникает потребность в формировании стандартизированных и единообразных систем хранения данной информации. Данный вопрос помогает решить разработка специализированных медицинских информационных систем.

Медицинская информационная система отличается от других программных продуктов, прежде всего тем, что в ней хранится и обрабатывается персональная и конфиденциальная информация. В связи с этим к ним выдвигаются повышенные требования к достоверности и ограничениям доступа к информации, юридической ответственности, техническим мерам защиты данных. Любой пользователь, получающий доступ к медицинской информационной системе, несет полную ответственность за конфиденциальность информации, которую он вносит, использует или передает другим пользователям.

Методы защиты информации в медицинских информационных системах. На данный момент в медицинских информационных системах стоит вопрос безопасности информации в двух точках зрения:

– защита прав личности от распространения конфиденциальной информации;

– защита интересов государства и ведомств. Возможность утечки информации, злоупотребление, нарушение этики.

– исходя из указанных требований для обеспечения защиты информации и программ медицинских информационных систем должны применяться следующие средства [1]:

– правовые;

– организационно-административные;

– технические (аппаратно-программные).

Правовые средства препятствуют несанкционированному использованию информации и являются сдерживающим фактором для потенциальных нарушителей.

Сюда нужно отнести те права и обязанности по получению, обработке, ограничению в распространении информации, которые прописаны в законодательной базе государства, которому подчиняется действия по работе с медицинской информационной системой.

Для обеспечения информации, этой законодательной базе должны подчинятся как медицинские информационные системы, так и все участники принимающие участия в работе с ней.

Организационно-административные средства регламентируют процессы функционирования медицинских информационных систем, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой и пользователей с администраторами системы.

Исходя из этого, в медицинских информационных системах должна быть выстроена иерархия ролей, каждая из который соотносится под различными должностями медицинских работников, сфер их деятельности, а также роли пациента. Каждая из таких ролей должна иметь ряд своих уникальных прав на взаимодействие с системой. Данное разграничение, служит для допуска к той части информации, которая соответствует компетенции пользователя. Данная особенность реализуется через технические средства защиты, и регламентируется правовыми средствами.

Технические средства выполняют следующие функции защиты: создание препятствий на возможных путях проникновения и доступа потенциальных нарушителей к медицинской информационной системе, идентификацию и авторизацию пользователей, разграничение прав доступа к ресурсам, регистрацию событий, криптографическую защиту информации [2].

Программно-технические меры системы безопасности медицинских информационных систем должны предоставлять средства распределения прав доступа, гарантируя возможность получения доступа пользователя только к той информации и программам, которые необходимы для выполнения функциональных обязанностей. Эти средства традиционно используют понятия:

– авторизация пользователя (технологии, подтверждающей, что реальный пользователь и персона, от чьего имени открывается доступ – одно и тоже лицо);

– группы доступа (логического объединения пользователей в одну группу, для которой система предоставляет одинаковые права);

– права доступа (различия в возможностях работы с медицинской информационной системой, например – чтение информации и изменение данных, удаление документов или даже модификацию программного кода);

– списка контроля доступа (таблица, объединяющая группы доступа и сопоставленные им уровни прав для конкретного объекта системы).

Алгоритм распределения прав доступа. Алгоритм работы технологии распределения прав доступа в медицинской информационной системы выглядит следующим образом:

– При старте системы выполняется авторизация пользователя. Для авторизации, зачастую используется связка логин-пароль, где логин идентифицирует пользователя, а пароль является средством подтверждения личности. При этом пароль должен быть представлен в зашифрованном виде, при хранении в системе. Наиболее часто используемые алгоритмы AES, DES, Blowfish и другие. По мимо этого, при работе по сети, необходимо обеспечить передачу пароля по защищенным протоколам, такими как SSL – протокол передачи информации, использующий асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений [3].

– В момент первого после авторизации обращения к серверу создается сеанс связи с сервером. Во время инициализации сеанса система определяет, в какие группы данный пользователь входит и однозначно ассоциирует пользователя с этими группами. Все дальнейшие действия в системе, включая открытие БД, отображение ее элементов дизайна или других программных элементов, осуществляться только исходя из текущего списка групп доступа.

– При последовательном запросе клиентом объектов системы на стороне сервера осуществляется проверка на наличие или отсутствие необходимых прав доступа к объекту. Если ни одна из групп пользователя не включена в объект, то сервер не предоставляет клиенту информации о наличии и свойствах объекта. Учитывая высший приоритет системы безопасности, несанкционированный доступ к такому объекту (серверу, БД, представлению, программе, документу или отдельно взятому полю) становиться теоретически и практически невозможным.

– При этом в системе на уровне ядра предусмотрены функции протоколирования несанкционированного доступа и программной обработки исключительных ситуаций в коде системы, которые одновременно позволяют администратору видеть все подозрительные с точки зрения безопасности запросы и, с другой стороны, обеспечивают требуемый уровень стабильности и производительности работы приложений системы.

Помимо распределения прав доступа, программно-технические меры системы безопасности должны предусматривать шифрование различной текстовой информации, а также мультимедии. Различные мультимедийные данные должны хранится в двоичном виде в базе данных с учетом алгоритмов шифрования, и представляется пользователю в виде расшифрованных данных в интерфейсе.

Заключение. Описанные технические, нормативные и иные средства обеспечения безопасности на сегодняшний день позволяют медицинским информационным системам обеспечивать весь необходимый комплекс мер защиты информации и программ, что является необходимым условием пригодности таких систем к их эксплуатации.

ЛИТЕРАТУРА

1. Информационные технологии в экономике. Методы и средства защиты информации. Авторы: Моисеенко Е.В., Лаврушина Е.Г., редактор: Л.З. Анипко, с. 25–30.
2. Cyberleninka.ru [Электронный ресурс]. Режим доступа: h https://cyberleninka.ru/article/n/algoritmy-i-tehnologii-obespecheniya-bezopasnosti-informatsii-v-meditsinskoy-informatsionnoy-sisteme-externet. – Дата доступа: 25.09.2019.
3. SSL протокол [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/SSL. – Дата доступа: 25.09.2019.