информационные технологии

Телемедицине не хватает защиты

с13

Медицинские организации, использующие компоненты телемедицины, обязаны обеспечить защиту системы от несанкционированного доступа и вирусных атак, а также защиту каналов передачи данных, внедрить решения для обнаружения вторжений и анализа надежности. Для идентификации пациентов должна использоваться единая система идентификации и аутентификации на Госуслугах, документирование информации об оказании медицинской помощи пациенту с применением телемедицинских технологий должно осуществляться с использованием усиленной квалифицированной электронной подписи, сообщает директор «ИТ Энигма Уфа» Александр Оводов и в то же время отмечает, что в защите есть пробелы.

«Телемедицина — это стремительно развивающийся рынок, на него выходит большое количество компаний и сервисов. Разрабатываются такие сервисы и приложения в большинстве своем без учета требований к обеспечению информационной безопасности. В результате разработанное программное обеспечение, приложения для мобильных устройств имеют уязвимости, которыми пользуются злоумышленники. Кроме того, многие компании, эксплуатирующие телемедицинские сервисы, не знают о требованиях информационной безопасности или частично их игнорируют. В результате становятся легкой мишенью злоумышленников, которые незаконно получают персональные данные пациентов и продают их на черном рынке или используют против пациентов. Яркие свежие примеры недостаточной защищенности персональных данных пациентов — базы данных двух крупных телемедицинских сервисов оказались в открытом доступе. Кроме того, при передаче организации обязаны использовать сертифицированные ФСБ средства криптографической защиты информации. Еще несколько лет назад на рынке не было сертифицированных решений, которые бы могли обеспечивать безопасность передачи данных между врачами и пациентами без покупки пациентами средств криптографической защиты информации. Сейчас такие решения есть, но используют их единицы», — отмечает он.

Иван Працкевич, специалист компании Mindray-shop.ru, занимающейся поставкой интеграций и разработкой системных решений для медицины отмечает, что помимо утечек данных пациентов, злоумышленники могут получить контроль и над медицинским оборудованием. «Пример — больница из небольшого города республики хочет показать федеральному центру данные своего пациента. Допустим, чудо — и в ЦРБ есть DICOM (Digital Imaging and Communications in Medicine — медицинский отраслевой стандарт создания, хранения, передачи и визуализации цифровых медицинских изображений и документов обследованных пациентов, — прим. «ИТ»), и мы можем отправить снимки КТ, рентген, МРТ, УЗИ-исследования. Может, даже настроена LIS (Laboratory information system — лабораторно-информационная система, прим. «ИТ»), и тогда есть доступ к анализам, которые были сделаны или назначены. Но в 99% случаев консультация ограничится письмом по электронной почте. В удаленных районах республики, для которых телемедицина необходима в первую очередь, отсутствуют элементарно специалисты, способные работать на современном оборудовании. После запуска всего этого механизма в массовом порядке, безусловно, необходим специальный канал передачи информации. Так как в противном случае, используя сеть WI-FI для посетителей, можно получить доступ не только в раздел с персональными данными, LIS-диагнозами и назначениями, но и взаимодействовать с критически важными системами наркозно-дыхательной аппаратуры, инфузионными системами, техникой для искусственного кровообращения и т.п. На сегодня наши клиники не готовы к подобному типу угроз полностью».

ОЛЕГ ХАРСЕЕВ

В условиях законодательных пробелов следить за защитой персональных данных должны прежде всего сами клиники

Рассчитывать на собственные силы

Опрошенные «ИТ» эксперты отмечают, что для развития защиты персональных данных в телемедицине необходимо принять соответствующие законодательные акты — действующих недостаточно.

В Роскомнадзоре планируют рассмотреть вопрос нормативного установления заданных параметров качества связи в сегментах, связанных с обеспечением жизни и здоровья человека. Начальник Управления контроля и надзора в сфере связи Роскомнадзора Денис Пальцин отметил, что вопросы качества оказываемых в Российской Федерации услуг связи, в медицинской среде нормативно-правовыми актами не урегулированы, поскольку были выведены из-под регулирования и отданы конкурентному рынку в период конца 80-х — начала 90-х годов.

Однако вопрос совершенствования нормативной базы может оказаться намного шире одной только сферы телемедицины. По мнению руководителя отдела Департамента информационной безопасности ООО «Сервионика» Александра Сальникова, удаленный мониторинг здоровья с использованием медицинских приборов соответствует парадигме «Интернета вещей», для которого российских стандартов пока нет. «На сегодня, пожалуй, единственным прикладным отраслевым документом в области защиты информации в медицине, не считая общеизвестных и частично устаревших ГОСТов, являются «Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости» от 2009 года. Их явно недостаточно с учетом современного развития информационных технологий. Отстают от современных ИТ-реалий и нормы регулирования в области телемедицины: отраслевого стандарта по информационной безопасности для этой сферы пока нет», — считает он.

В ситуации законодательных пробелов, следить за сохранностью информации должны, прежде всего, сами клиники. Юрист Александр Болдырев отмечает, что каждое медицинское учреждение должно иметь серьезный набор внутренних нормативных документов и средств защиты информации на случай хранения, обработки и передачи персональных данных пациентов. Должен быть назначен сотрудник, непосредственно и лично отвечающий за их сохранность, считает он.

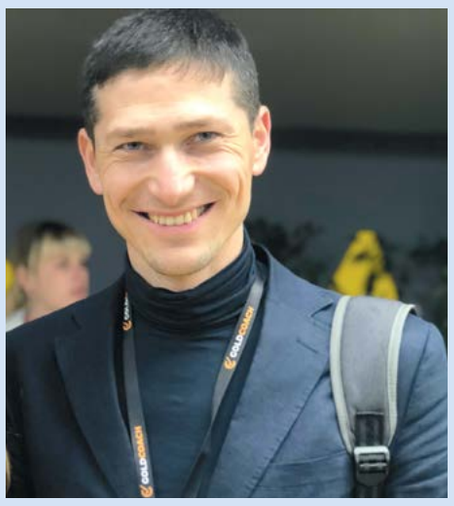
«Кибербезопасность обеспечить не очень сложно. Есть области, где комплекс мер по соблюдению безопасности опережает медицину, например, банковская сфера. И опыт отраслей-передовиков может быть применим и к здравоохранению. Есть прямая корреляция между применяемым комплексом мер по защите персональной информации, ценностью этих данных и возможными негативными последствиями для субъектов персональных данных, если они попадут к злоумышленникам. В России ценность персональных медицинских данных не очень высока по сравнению с другими развитыми странами. И возможные негативные последствия в России сравнительно ниже. Например, в ряде стран стоимость медицинского полиса напрямую зависит от состояния здоровья пациента, и утечка персональных медицинских данных может существенно сказаться на стоимости полиса. Например, наличие онкологического заболевания может быть косвенно причиной в отказе приема на работу. Сейчас мы проходим этап осознания ценности персональных медицинских данных и оценки возможных рисков в случае их утечки. Осознавая возможные последствия, мы предъявляем все более жесткие требования к защите личной информации, совершенствуем законодательную базу», — подчеркивает глава отдела цифрового здравоохранения компании Philips в России и СНГ Сергей Лаванов.

Лида Богатырева

ЦИФРОВАЯ МЕДИЦИНА

Как обеспечить безопасность данных пациентов

При строительстве, модернизации и эксплуатации медицинских объектов, телемедицинских сервисов важно учитывать необходимость обеспечения информационной безопасности. Директор компании «ИТ Энигма Уфа» Александр Оводов рассказал о требованиях к системам безопасности в медицинской отрасли, чем грозит отсутствие их соблюдения, и почему важно об этом задумываться еще на этапе составления бизнес-плана и проектирования.



— Сейчас медицинская отрасль не такая, как раньше. Почему, на ваш взгляд, так важна информатизация в этой сфере?

— Понятно, что современная медицина немыслима без использования информационных технологий — это и медицинские информационные системы, цифровое лабораторное оборудование, компьютерная томография, аппараты УЗИ, средства мониторинга состояния пациента, медицинское оборудование, используемое при проведении медицинских вмешательств, средства и сервисы дистанционного консультирования пациентов и даже 3D-принтеры. Построенные и проектируемые сейчас современные клиники уже оборудуются цифровыми автоматизированными системами жизнеобеспечения и мониторинга состояния пациентов; системами вентиляции, кондиционирования, управления освещением, температурой в помещениях. Все указанные информационные системы, автоматизированные системы управления и объединяющие их сети являются объектами информационной инфраструктуры организации.

— Расскажите, пожалуйста, как регулируется кибербезопасность в медицине?

— Помимо обеспечения безопасности персональных данных (152-ФЗ) появилась необходимость обеспечивать защиту информационной инфраструктуры. Она должна осуществляться в соответствии с 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» и подзаконными актами. К сожалению, на практике, медицинские организации не знают всего объема требований по информационной безопасности, которые им необходимо выполнить, не говоря уже о их реализации. Если взять 152-ФЗ, то «за кадром» часто остаются Постановление Правительства №1119, Приказ ФСТЭК №21, Приказ ФСБ №378. Для 187-ФЗ — это Постановление Правительства №127, Приказы ФСТЭК 229, 235, 236, 239, Приказы ФСБ 366, 367, 368.

— Чем грозит их невыполнение?

— Невыполнение требований может привести не только к административной ответственности и штрафам, уже измеряющимися сотнями тысяч рублей, но и к уголовной. В частности, одновременно с 187-ФЗ были внесены изменения в Уголовный Кодекс Российской Федерации и введена уголовная ответственность на срок до шести лет лишения свободы при нарушении правил эксплуатации и правил доступа к персональным данным пациентам, если оно повлекло причинение вреда, и на срок до 10 лет при тяжких последствиях.

— Что произойдет если не учесть требования информационной безопасности на этапе проектирования?

— Во-первых, затраты на построение системы защиты информации, ее эксплуатацию, не будут заложены в финансовую модель. Как следствие расчеты рентабельности, срок возврата инвестиций, срок выхода на точку безубыточности будут определены некорректно. Во-вторых, может потребоваться изменение топологии локальной сети, и, как следствие, проведение дополнительных строительных работ. В-третьих, могут потребоваться дополнительные серверные и телекоммуникационные шкафы под размещение программно-аппаратных комплексов средств защиты информации, источников бесперебойного питания. В-четвертых, может потребоваться увеличение или изменения конфигурации серверов и рабочих мест пользователей.

— Как можно избежать этих затрат?

— Избыточных затрат можно избежать, если проектировать систему защиты информации одновременно с выбором информационных систем, медицинского оборудования, автоматизированных систем управления.

— А что делать, если медицинская клиника уже функционирует?

— Для действующих медицинских организаций необходимо в срок до 1 сентября 2019 года провести работы по определению объектов информационных инфраструктур, подлежащих категорированию в соответствии с 187-ФЗ, затем направить их перечень во ФСТЭК России. Дальше уже проводить категорирование объектов, проектировать и строить систему защиты.

— Какие есть особенности при онлайн-взаимодействии медицинской организации с клиентами?

— Если организация выходит в онлайн взаимодействие с клиентом, то особое внимание следует уделить защите сайта и мобильного приложения. Необходимо применять специализированные межсетевые экраны для веб-приложений, осуществлять анализ исходного кода приложений на отсутствие уязвимостей, озаботиться внедрением отечественных средств криптографической защиты информации в приложения и сайты для защиты передаваемых данных, периодические проводить анализ защищенности. Если этого не делать, доступ к персональным данным может оказаться в открытом доступе, как например, это произошло в марте с телемедицинским сервисом DOC+ и в апреле с CMD.

— Как быть организациям, которые оказывают телемедицинские услуги?

— На них распространяются те же требования, что и на медицинские организации, которые выходят на онлайн-взаимодействие с клиентами.

— Может ли в этом помочь ваша компания?

— Да, можем. На этапе разработки инвестиционных проектов можем провести оценку исходных данных и сделать расчет стоимости системы защиты. На этапе проектирования, как лицензиаты ФСТЭК и ФСБ, готовы осуществить разработку проектных решений на систему защиты. На этапе ввода в эксплуатацию и для работающих клиник осуществить внедрение средств защиты информации, разработку организационно-распорядительных документов, провести анализ защищенности всей информационной инфраструктуры.

На этапе эксплуатации взять на себя все заботы обеспечения информационной безопасности — от сопровождения средств защиты информации до взаимодействия с регуляторами (Роскомнадзором, ФСТЭК, ФСБ). Для онлайн-сервисов осуществляем приемку исходного кода приложений на соответствие требованиям информационной безопасности (поиск уязвимостей в коде).