безопасность цифровой медицинской среды

Федотова Г.В., д.э.н., доцент,

ФИЦ ИУ РАН, г. Москва, Россия

Новицкая О.С., директор,

Оренбургский филиал ООО «Капитал МС», г. Оренбург, Россия

Аннотация. В статье рассмотрены проблемы потери данных, связанные с дестабилизацией работы интернет-сервисов вследствие атак хакеров на критическую инфраструктуру, в том числе в сфере здравоохранения. Приведены масштабы финансовых потерь вследствие утечек данных пациентов.

Ключевые слова: безопасность, цифровая среда, медицинские услуги, цифровая безопасность.

Цифровые медицинские контуры учреждений здравоохранения были спроектированы в рамках реализации Национального проекта «Здравоохранение», который к концу 2024 году завершается. При этом функционирующие цифровые контуры медицинских организаций будут поддерживаться новыми проектами в сфере здравоохранения.

К примеру, в 2025 году стартует Национальный проект «Продолжительная и активная жизнь», в рамках которого поставлена генеральная цель – увеличение здорового долголетия граждан до 80 лет. Основными инструментами достижения цели выступают – ранее диагностирование заболеваний, развитие медицинской инфраструктуры, цифровой персонализированный подход к пациентам.

В этой ситуации выстроенные цифровые контуры пациентов в медицинских организациях дают возможность для мгновенной обработки данных и формирования Дата-центров информации о пациентах и динамики их состояния здоровья. Накопленные информационные ресурсы формируют базу для медицинской статистики на конкретной территории и закладываются в основу будущего бюджетного планирования расходов на здравоохранение.

Информационные ресурсы медицинских организаций – это наиболее привлекательный объект атак кибермошенников, стремящихся заработать на утечке персональных данных или дестабилизировать работу критической цифровой инфраструктуры России [1]. Хранящиеся персональные данные, данные о платёжных картах, страховых полисах, информация о страховых выплатах пациентам - все это привлекательный товар для

хакеров, работающих в цифровой среде и имеющий спрос в DarkNet [2].

Согласно статистике от различных поставщиков информационных технологий защиты по данным 2023 года количество успешных атак на медицинские организации возросла на 78%, за первую половину 2024 года по сравнению с аналогичным периодом 2023 года рост составил 32%, что выступает тревожным фактором и инструментом для стресс-тестирования систем безопасности цифровых медицинских платформ.

Отнесение медицинской информационной инфраструктуры к критической налагает определённую ответственность на учреждения и организации, поэтому в рамках исполнения Указа Президента РФ от 30.03.2022 № 166 до 1 января 2025 годы они будут мигрировать на отечественные ПО.

Информация медицинских баз данных включает не только персональные данные по пациентам, но также данные о выплатах компенсационного характера от страховых компаний, сведения о личных счетах, поэтому хакеры активно эксплуатируют уязвимости медицинских сервисов для краж и последующего шантажа. Среди критических хакерских атак на медицинские сервисы данные организации занимают лидирующие позиции.

Однозначно, что медицинские организации самостоятельно с данной проблемой не справятся без государственной поддержки со стороны специализированных служб. Поэтому помимо цифрового контура необходимо дополнительно строить контур информационной безопасности с привлечением специалистов. Вопросы безопасности медицинского контура – вопросы государственной безопасности, так как именно государство гарантирует своим гражданам тайну и неприкосновенность личной и семейной жизни согласно ст. 23 Конституции РФ [3].

Конституционные гарантии гражданам обеспечиваются специальными службами, работающими по линии государственной безопасности. Так, в НИИ организации здрав оохранения и медицинского менеджмента было учреждено новое подразделение – управлении информатизации. Функционал данного структурного органа сводится к информационной поддержке всех медицинских организаций г. Москвы (249 учреждений) и своевременной помощи при возникновении критических ситуаций. Отнесение организаций здравоохранения к объектам критической информационной инфраструктуры России дает дополнительные преимущества в плане технологической поддержки и консультирования по вопросам защиты персональных медицинских данных и устойчивости цифрового медицинского контура.

Подразделение получило лицензию Федеральной службы по техническому и экспертному контролю РФ и совместно организовывает работы по таким направлениям:

-категорирование объектов цифровой инфраструктуры,

-стандарты и требования по защите цифровых сервисов,

-разработка программ повышения квалификации для IT-специалистов.

Таким образом, завершая наше исследование отметим, что выстраивание информационной защиты цифрового медицинского контура – это важная задача, которая должна быть решена как средствами медицинской организации, так и средствами государственного специализированного сектора.

Последствия успешных хакерских атак на медицинскую инфраструктуру влекут за собой не только репутационные, но и финансовые потери для медицинских организаций, связанные с расходами на восстановление работы инфраструктуры и баз данных, выплаты выкупа шантажистам и компенсации издержек пациентам. По данной причине финансовая безопасность при реализации проектов цифровизации в здравоохранении должна быть продумана в первую очередь.

Литература

1. Федотова А.М. Актуальные проблемы современной медицинской науки в России // Актуальные проблемы экспериментальной и клинической медицины: Сборник статей Международной научно-практической конференции. Волгоград, 2023. С. 419-420.

2. Козенко Т.Е., Федотова А.М. Блокчейн-технологии в цифровом профиле пациента // Прикладные экономические исследования. 2022. № 4. С. 51-56.

3. Орлова Е.Р., Бочарова И.Е., Козенко Т.Е., Федотова А.М. Основные направления цифровизации в области здравоохранения // Информационные технологии и вычислительные системы. 2023. № 2. С. 18-26.