УДК 330.3

Т.Н. Беляцкая, к.э.н., доцент, зав.каф. менеджмента УО БГУИР
О.М. Маклакова, ст.преп. каф.менеджмента УО БГУИР

Электронное здравоохранение в контексте национальной безопасности Республики Беларусь

Развитие электронного здравоохранения является одним из приоритетных направлений цифровизации в Республике Беларусь. Старение населения Беларуси вызвано рядом факторов, в первую очередь проблемами возобновления населения и увеличением продолжительности жизни. Такая же тенденция характерна для Европы и США и других развитых регионов. Данная тенденция приводит к росту затрат на подержание здоровья стареющегонаселения. Эти затраты в большинстве европейских стран являются растущей составляющей ВВП, а в некоторых случаях все еще растущей частью государственных финансов, составляющей от 4% до 12% ВВП в государствах-членах ЕС.Более 70% бюджета на здравоохранение расходуется на хронические заболевания. И эта цифра растет.В Республике Беларусь расходы на здравоохранение составляют 4, 6 % от ВВП.

Ожидается, что использование возможностей электронного здравоохранения позволит не только значительно ускорить и сделать доступным персонализированный удаленный уход за пожилыми и хронически больными, но и удешевить его в перспективе.

Однако кроме ожидаемых эффектов положительного характера необходимо тщательно проанализироватьэти тенденции с точки зрения обеспечения безопасности конкретных участников системы электронного здравоохранения и национальной безопасности в целом.

Имеющиеся угрозы следует разделить на две группы, используя критерий наличие / отсутствие внедрения систем электронного здравоохранения.

Промедление развертывания систем электронного здравоохранения приведет к развитию проблем в области экономической безопасности – значительное удорожание стоимости обеспечения услуг здравоохранения; в области демографической безопасности – ухудшение демографических показателей вследствие снижения доступности и качества оказания услуг здравоохранения.

В свою очередь развертывание систем электронного здравоохранения поднимает проблемы в области технической безопасности, такие как зависимость от платформ, обеспечивающих хранение персональных медицинских данных, а также информационной безопасности, связанной с киберпреступностью.

Проблема кибербезопасностисостоит в том, что персонализация информации о пациенте и его истории болезни, мониторинг сигналов состояния здоровья пациента и, главное, хранение всех этих данных и обеспечение их обмена в целях оказания медицинских услуг увеличиваетриски потери конфиденциальности.

Действительность информационного общества демонстрирует постоянное возрастание числа и многообразия форм кибератак.Кибератаки фокусируются в основном на краже финансовой, платежной информации и номеров банковских счетов с использованием украденных устройств снезашифрованными данными, фишинг и спам. Технологические достижения привели к продвинутой кибервойне с использованием SQL-инъекций, продвинутых постоянных угроз, наличие уязвимости нулевого дняатаки и вредоносных программ.

Сфера электронного здравоохранения не является исключением. Отсутствие адекватных расходов на ИТ со стороны организаций здравоохранения и недостаточная осведомленность о киберпреступности выявили уязвимостиорганизаций. Ущербкибератакв мировом масштабе

насистемы здравоохранения в целом оценивается почти в шесть миллиардов долларов в год.

Кроме того, организации здравоохранения сталкиваются с конкретными угрозами из-за таких факторов, как использованиеоблачных сервисов, небезопасных сетей, халатности сотрудников, использование сотрудниками и пациентами собственных устройств (BYOD– bringyourowndevice), отсутствие внутренней идентификации и систем безопасности, кража устройства с незашифрованными данными и др.

Критически важным является обеспечение гарантийкибербезопасностиуже на стадии проектирования, разработки, а также эксплуатации устройств и систем электронного здравоохранения. Кроме того, каждый участник сектора электронного здравоохранения имеет конкретные потребности и требования кибербезопасности, которые в некоторых случаях могут вступать в конфликт. Поэтомуважно собрать полные и всесторонние требования кибербезопасности от каждой группы.

Для пациентов в области безопасности важныобеспечение конфиденциальности личной информации иобеспечение устойчивости (безотказности систем, доступ в режиме реального времени) услуг электронного здравоохранения.

Требования врачей и других медицинских работников состоят в прозрачности, простоте использования и доступности информации. Эти требования в некоторой степени противоречат желанию пациентов соблюдать конфиденциальность и распоряжаться данными по своему усмотрению.

Одним из ключевых интересовфармацевтических компанийявляется наличие информации о пациентах, необходимой для проведения исследований и испытаний, что также может противоречить потребностям самих пациентов.

Основные требования производителей медицинских приборов и прочих информационно-коммуникационных технологий (ИКТ) для медицины –

устойчивостьсистем здравоохранения, под которой подразумевается доступность данных в режиме реального времени. Другая существенная потребность – полная уверенность в целостности и достоверностиинформации, которой управляют, поскольку ложные данные могут привести к ошибочным исследованиям, неправильной диагностике и, в конечном итоге, даже к серьезным угрозамздоровью пациентов. Еще одна существенная потребность в сфере здравоохранения – это необходимость обеспечить довериепациентов в том, что их информация обрабатывается ответственно.

Исходя из вышеизложенного, обеспечение национальной безопасности в сфере электронного здравоохранения требует реализации следующих направлений развития:

1 устойчивостисистемы электронного здравоохранения к кибератакам, предотвращение утечки и потери данных;

2обеспечение мониторинга безопасности и надежности в режиме реального времени;

3обеспечение осведомленности персонала об основных угрозах кибербезопасности, что требует повышение навыков - как технических, так и поведенческих - персонала посредствоминновационных методов обучения;

4доступность системы электронного здравоохранения и непрерывность процессов для обеспечения бесперебойногооказания услуг электронного здравоохранения;

5 обеспечение безопасности, целостности и достоверности данных;

6. прозрачность использования данных медицинскими работниками всех категорий, фармацевтами и исследователями;

7 гармонизация стандартов, законовв области оказания услуг здравоохранения в целом и электронного здравоохранения, в частности.

Список литературы:

1 Беляцкая, Т.Н., Маклакова, О.М. Готовность населения к экономическому поведению в условиях электронной экономики: проблемы электронного здравоохранения // Цифровая трансформация: 2019, № 2 (7), С.13-28

2 Шандора, Н.И., Полоник И.С. Факторы развития и совершенствования системы здравоохранения Республики Беларусь // Новая экономика: 2019, № 1 (73), С.97-106

3 HEALTH CARE AND CYBER SECURITY: Increasing Threats Require Increased Capabilities / [Электронныйресурс]. – 2019. – Режимдоступа: https://assets.kpmg/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf. – Датадоступа: 01.10.2019.

4 HEALTHCARE SECTOR REPORT / [Электронный ресурс]. – 2019. – Режим доступа: https://www.ecs-org.eu/documents/publications/5ad7266dc1cba.pdf. – Дата доступа: 01.10.2019.

5 Бюджет Республики Беларусь на 2019 год для граждан / [Электронныйресурс]. – 2019. – Режимдоступа: http://www.minfin.gov.by/upload/bp/budjet/budjet2019.pdf. – Дата доступа: 01.10.2019.

6 Безкоровайный, М.М., Татузов, А.Л. Кибербезопасность: подходы к определению понятия / Вопросы кибербезопасности №1(2) – 2014. – [Электронныйресурс]. – 2014. – Режимдоступа: https://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya– Дата доступа: 04.10.2019.