



Готовность объектов здравоохранения к 1 января 2025 г.: проблемные вопросы

Начальник отдела информационной безопасности
ФГБНУ «РНЦХ им. акад. Б.В. Петровского»
Хлопотников Алексей Леонидович

Переход на отечественное программное обеспечение

В свете последних событий, связанных с санкциями и необходимостью импортозамещения, вопрос готовности объектов здравоохранения к переходу на отечественное программное обеспечение становится все более актуальным. 1 января 2025 года является важной контрольной точкой, к которой все объекты здравоохранения должны быть готовы к полному переходу на отечественные программные продукты и решения. Однако на пути этого перехода возникают ряд проблемных вопросов, которые требуют детального рассмотрения и анализа.



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации

В целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации **п о с т а н о в л я ю:**

1. Установить, что:

а) с 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" (далее - заказчики), не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов (далее - программное обеспечение), в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура), а также закупки услуг, необходимых для использования этого программного обеспечения на таких объектах, без согласования возможности осуществления закупок с федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации;

б) с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.



2 100068 22761 1

Текущее состояние информатизации здравоохранения



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 1 июня 2021 г. № 852

МОСКВА

О лицензировании медицинской деятельности (за исключением указанной деятельности, осуществляемой медицинскими организациями и другими организациями, входящими в частную систему здравоохранения, на территории инновационного центра "Сколково") и признании утратившими силу некоторых актов Правительства Российской Федерации

В соответствии с Федеральным законом "О лицензировании отдельных видов деятельности" Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые:

Положение о лицензировании медицинской деятельности (за исключением указанной деятельности, осуществляемой медицинскими организациями и другими организациями, входящими в частную систему здравоохранения, на территории инновационного центра "Сколково");
перечень тождественных работ (услуг), составляющих медицинскую деятельность.

2. Выданные до дня вступления в силу настоящего постановления лицензии на осуществление медицинской деятельности подлежат переоформлению в части исключения работ (услуг), не предусмотренных приложением к Положению, утвержденному настоящим постановлением, не позднее чем до 1 сентября 2022 г., за исключением тождественных работ (услуг), составляющих медицинскую деятельность, предусмотренных перечнем, утвержденным настоящим постановлением.

Неравномерное внедрение информационных систем (ИС)

- В разных регионах и даже отдельных учреждениях уровень информатизации существенно отличается.
- Существует множество региональных МИС (медицинских информационных систем): МИС БАРС, МИС ЕМИАС, МИС ИС Медицина, МИС Инфоклиника и много других.
- Согласно Постановлению Правительства Российской Федерации от 01.06.2021 № 852 "О лицензировании медицинской деятельности (за исключением указанной деятельности, осуществляемой медицинскими организациями и другими организациями, входящими в частную систему здравоохранения, на территории инновационного центра "Сколково") и признании утратившими силу некоторых актов Правительства Российской Федерации" **Медицинские организации обязаны отправлять сведения о своих пациентах в ЕГИСЗ подсистему РЭМД (реестр электронной медицинской документации)**

Текущее состояние информатизации здравоохранения



Использование зарубежного ПО

Значительная часть медицинских учреждений использует зарубежное программное обеспечение, что создает риски зависимости от иностранных вендоров.

Кроме того, для большинства используемых медицинских систем, базирующихся на иностранном ПО, просто нет отечественных заменителей. Особенно это касается оборудования для оказания высокотехнологичных медицинских услуг таких как МРТ, ПЭТ КТ, роботизированные медицинские комплексы. Это может привести к тому, что дорогостоящие комплексы в какой-то момент просто перестанут работать.

Текущее состояние информатизации здравоохранения

Низкий уровень интеграции

Существующие ИС часто несовместимы между собой, что затрудняет обмен данными и снижает эффективность работы. Это обусловлено:

- различия в стандартах и протоколах передачи данных;
- отсутствие единых требований к МИС;
- недостаточное финансирование для развития и внедрения МИС;
- обеспечение подготовки специалистов в области информационных технологий и здравоохранения;
- низкий обмен опытом и лучшими практиками между регионами.

Проблемные вопросы перехода на отечественное ПО

Функциональность и совместимость


- Отечественное ПО должно быть функционально эквивалентно зарубежным аналогам и обеспечивать совместимость с существующими ИС.
- Функционал ПО включает в себя различные аспекты, такие как диагностика, лечение, мониторинг пациентов, управление медицинскими учреждениями и т.д.
- Совместимость означает возможность взаимодействия различных систем между собой, обмен данными и информацией.

Проблемные вопросы перехода на отечественное ПО

Безопасность и надежность

Важным аспектом является также обеспечение информационной безопасности и защиты персональных данных пациентов.

- ПО должно соответствовать высоким требованиям безопасности и надежности, гарантируя в том числе, сохранность персональных данных пациентов.
- Нарушение конфиденциальности может привести к серьезным последствиям для пациентов и медицинских учреждений.
- Для обеспечения информационной безопасности необходимо использовать надежные системы защиты данных, такие как шифрование, аутентификация пользователей и контроль доступа к информации.
- Соблюдение приказов ФСТЭК 17, 21, 31, 235, 239 по защите информации, а также Федеральных законов 187 ФЗ, 149 ФЗ, 152 ФЗ, 63 ФЗ.



Проблемные вопросы перехода на отечественное ПО

Финансовые затраты

Переход на новое ПО требует инвестиций в закупку лицензий, обучение персонала и возможную модернизацию инфраструктуры.

Построение системы защиты информации на объектах информатизации требуют также больших финансовых затрат которые ложатся на медицинские организации, и очень часто выполняются только формально.

Проблемные вопросы перехода на отечественное ПО

Кадровый потенциал

Недостаток квалифицированных специалистов, способных работать с отечественным ПО, может стать серьезным препятствием.

Недостаток специалистов по защите информации в медицинских организациях, эта проблема на данный момент стоит особенно остро в текущих условиях, когда важно обеспечить хранение данных на территории РФ, а значит выбирать российские программные решения, независимые от зарубежных поставщиков.

Особое внимание стоит уделить защите объектов критической информационной инфраструктуры, так как сфера здравоохранения относится к объектам КИИ.

Требования к специалистам обеспечивающим безопасность КИИ регламентируются как Указом президента № 250, так и приказами ФСТЭК для ЗОКИИ.

Проблемные вопросы перехода на отечественное ПО


Кадровый потенциал

Недостаток квалифицированных специалистов, способных работать с отечественным ПО, может стать серьезным препятствием.

Недостаток специалистов по защите информации в медицинских организациях, эта проблема на данный момент стоит особенно остро в текущих условиях, когда важно обеспечить хранение данных на территории РФ, а значит выбирать российские программные решения, независимые от зарубежных поставщиков.

Особое внимание стоит уделить защите объектов критической информационной инфраструктуры, так как сфера здравоохранения относится к объектам КИИ.

Требования к специалистам обеспечивающим безопасность КИИ регламентируются как Указом президента № 250, так и приказами ФСТЭК для ЗОКИИ.



Проблемные вопросы перехода на отечественное ПО

Сопrotивление изменениям

При Внедрении нового ПО можно столкнуться с сопротивлением со стороны персонала, привыкшего к работе с существующим ПО.

Чтобы избежать этого, необходимо проводить обучение персонала и объяснять преимущества нового ПО.

Также возможно организовать переход на новое ПО постепенно, чтобы сотрудники могли привыкнуть к новым функциям и интерфейсу.

Пути решения проблем

Разработка и поддержка отечественного ПО

Необходимо стимулировать разработку конкурентоспособного отечественного ПО, отвечающего потребностям здравоохранения.

Внедрение отечественных операционных систем таких как: Astra Linux Special Edition, РЕД ОС, ALT Linux, которые имеют сертификаты ФСТЭК по защите информации и дружественный интерфейс.

Взаимодействие с поставщиками оборудования, для совместимости оборудования с отечественными операционными системами и программными продуктами включая МИС.

Государственная поддержка

Государство должно оказывать финансовую и организационную поддержку для разработки и перехода на отечественное ПО.

Пути решения проблем

Обучение и повышение квалификации

Необходимо организовать программы обучения эксплуатационного персонала работе с новым ПО, осуществлять подготовку как централизованно, рассказывая о возможностях того или иного ПО – аналога зарубежного, так и непосредственно обучая уже в медучреждениях, т.е. непосредственно на рабочем месте, на конкретных комплексах.

Специалисты по защите информации должны быть обучены работе с медицинскими данными и знать все особенности работы с ними. Они также должны знать, как защитить данные от различных угроз, таких как хакерские атаки, вирусная активность и другие угрозы.

Обучение специалистов по защите информации должны включать в себя курсы по информационной безопасности, тренинги по работе с системами защиты и реагирования на компьютерные угрозы. Особенности взаимодействия с НКЦКИ и ФСТЭК.

Пути решения проблем

Информационная кампания

Необходимо разъяснить медицинским работникам преимущества перехода на новое программное обеспечение.

Это может включать в себя:

- улучшение качества обслуживания пациентов;
- повышение эффективности работы медицинских учреждений;
- улучшение безопасности данных и защиты информации обрабатываемых в учреждениях

Также важно создать позитивный настрой у медицинского сообщества, чтобы они были готовы к переходу на новое ПО.



Заключение

Переход на отечественное программное обеспечение в сфере здравоохранения является сложным, но необходимым процессом. Для успешной реализации этой задачи необходимо разработать комплекс мер, которые будут учитывать все проблемы и пути их решения. Это включает в себя обеспечение функциональности и совместимости программного обеспечения, обеспечение информационной безопасности, обучение специалистов и создание позитивного настроения у медицинского сообщества. Только такой комплексный подход может обеспечить успешное внедрение отечественного программного обеспечения в сфере здравоохранения.



Спасибо за внимание!