Построение защищенной сети для автоматизированных систем управления лекарственным обеспечением населения

Лысков С.В.[1], Кошкаров А.А.[2], Кугаевский Д.Н.[1]
[1]Государственное унитарное предприятие Краснодарского края «Кубаньфармация»
[2]Кубанский государственный университет, Краснодар

Аннотация

В целях совершенствования процессов управления лекарственным обеспечением населения по отпуску медицинской продукции льготным категориям граждан актуальна задача выбора защищенных каналов связи для электронного взаимодействия. В работе приведено описание технологий построения защищенного обмена. Рассмотрены факторы выбора криптографических решений.

Интеграция информационных систем (ИС) всех участников организации льготного лекарственного обеспечения, главным образом медицинских и аптечных организаций регионов предполагает высокую скорость взаимодействия. Поэтому стала актуальной задача обновления автоматизированных систем управления лекарственным обеспечением населения и как следствие изменения системы обеспечения защиты данных, в том числе подсистемы шифрования.

Для защиты персональных данных отдельных категорий граждан от раскрытия, модификации и навязывания при информационном обмене между территориально удаленными пунктами отпуска медицинской продукции может применяться подсистема шифрования данных – Программный комплекс «Агава-СК» версии 1.0, или аналогичные средства криптографической защиты информации (СКЗИ). Агава-СК осуществляет шифрование выгруженной из базы информации, содержащей персональные данные, и формирует зашифрованные готовые к передаче файлы. Отправка зашифрованных файлов может быть осуществлена через любые каналы связи посредством сторонних программ приема-передачи информации. Условно такую схему передачи данных можно назвать «пакетной». Недостатками пакетного решения являются:

– отсутствие возможности установления доверительного и защищенного взаимодействия между субъектами и объектами доступа на уровне программных приложений и в реальном режиме времени;

– отсутствие возможности авторизации субъекта и объекта доступа;

– наличие многих звеньев передачи информации, что снижает надежность функционирования системы;

– отсутствие возможности гарантированной доставки данных;

– временные задержки в процессе обмена информацией между участниками.

Основными факторами, влияющими на выбор новой технологии обеспечения защищенного информационного взаимодействия, определены:

1. Наличие СКЗИ по уровню не ниже КС1 для нейтрализации атак без привлечения специалистов в области разработки и анализа СКЗИ, в соответствии с установленным уровнем защищенности ИС персональных данных и актуальными угрозами безопасности;
2. Наличие сертификатов соответствия ФСБ и ФСТЭК по требованиям безопасности для СКЗИ;
3. Устранение недостатков пакетной схемы передачи данных;
4. Обеспечение защиты каналов связи согласно методическим рекомендациям Министерства здравоохранения РФ для возможности дальнейшей интеграции с внешними системами и их взаимодействия.

На основе определенных факторов предложено решение в пользу продуктовой линейки компании ОАО «Инфотекс» для построения защищенной корпоративной сети передачи данных по технологии ViPNet. Такая технологическая схема не имеет недостатков пакетного решения, позволяет осуществить шифрование на сетевом уровне модели OSI и организовать виртуальную частную VPN-сеть.

Литература:

1. ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель».

2. Кошкаров А.А. Концепция интеграции систем выдачи и обслуживания льготных рецептов на территории Краснодарского края / А.А. Кошкаров, А.А. Халафян, А.Б. Семенов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2015. – №06(110). – IDA [article ID]: 1101506041. – Режимдоступа: http://ej.kubagro.ru/2015/06/pdf/41.pdf, 1,500 у.п.л.

3. Методические рекомендации медицинским организациям по обеспечению криптографической защиты каналов при взаимодействии в рамках единой государственной информационной системы в сфере здравоохранения [Электронный ресурс]. Режим доступа: http://portal.egisz.rosminzdrav.ru/files/Методические_Рекомендации_МЗ_v10_1.pdf (08.08.2016).

4. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5. Принципы маршрутизации и преобразования IP-трафика в VPN-сети, созданной с использованием технологии ViPNet [Электронный ресурс]. Режим доступа: https://www.infotecs.ru/press/publications/detail.php?ID=8633 (08.08.2016).

6. Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных».