7 декабря
2020

Онлайн-
конференция

РОССИЙСКАЯ
НЕДЕЛЯ ЗДРАВООХРАНЕНИЯ
RUSSIAN HEALTH CARE WEEK

Шестая Всероссийская конференция

АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ МЕДОРГАНИЗАЦИИ

ЭКСПОЦЕНТР
МЕЖДУНАРОДНЫЕ ВЫСТАВКИ И КОНГРЕССЫ
МОСКВА

forum imperia
КОНГРЕССНО — ВЫСТАВОЧНАЯ КОМПАНИЯ

PICOMEDICINE

Моя клиника – моя крепость.

Выстраивание системы защиты данных в медицинской организации

Игорь Борисенко

Создатель МИС «Цифровая клиника ПикоМедицина»

МИС и соответствие «Приказу МЗ РФ №911н»

МИС МО предназначены для сбора, хранения, обработки и представления информации, необходимой для автоматизации процессов оказания и учета медицинской помощи и информационной поддержки медицинских работников, включая информацию о пациентах, об оказываемой им медицинской помощи и о медицинской деятельности медицинских организаций

Глава I п. 3. Приказ МЗ РФ от 24.12.2018 № 911н

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

ФЗ от 27.07.2006 № 149-ФЗ «Об информационных технологиях и о защите информации»

Что же нужно «защищать»?

Информация, содержащаяся в информационных системах, подлежит защите в соответствии с законодательством РФ об информации, информационных технологиях и о защите информации и законодательством РФ в области персональных данных.

Защита информации, содержащейся в информационных системах, должна обеспечиваться посредством применения организационных и технических мер защиты информации.

Глава II п. 9. Приказ МЗ РФ от 24.12.2018 № 911н

МИС в терминах 911 приказа – это все сразу, что работает в вашей клинике

Требуется ли сертифицировать МИС

Программно-технические средства ИС должны … быть сертифицированными ФСБ РФ и (или) ФСТЭК в отношении входящих в их состав средств защиты информации, включающих программно-аппаратные средства, средства антивирусной и криптографической защиты информации и средства защиты информации ...

Глава II п. 9. Приказ МЗ РФ от 24.12.2018 № 911н

Контролируемая зона

Пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Границей контролируемой зоны может быть: периметр охраняемой территории подразделения (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения

Требования к медицинской информационной системе медицинской организации (МИС МО) https://portal.egisz.rosminzdrav.ru/materials/351

«Прикладной компонент» – те самые программы, которые называются МИСами, сертификации не требуют

Реальные угрозы безопасности

- **Остановка работы**
  - Квалификация персонала
  - Обрыв связи
  - Хакерские атаки
  - Вирусы
- **Утеря данных**
  - Надежность оборудования
  - Архивирование
  - Кому принадлежат данные в облаке
- **Утечки**
  - База данных ваших клиентов будет продана и им начнут звонить конкуренты
- **Несанкционированный доступ**
  - Одна учетная запись на всех
  - ЭЦП в тумбочке

Реальные угрозы безопасности

Антивирусы

- установите на всех компьютерах
- регулярно обновляйте

Архивирование

- организуйте обязательное архивирование сайта
- настройте архивирование базы

Взлом систем

- у каждого пользователя - свой пароль; создавайте сложные пароли
- не храните пароли в публичном доступе
- устанавливайте «заплатки»

Квалификация системного администратора

- должен изучать эксплуатационные документы МИС
- должен следовать рекомендациям разработчиков

Назначьте ответственных, контролируйте работу!

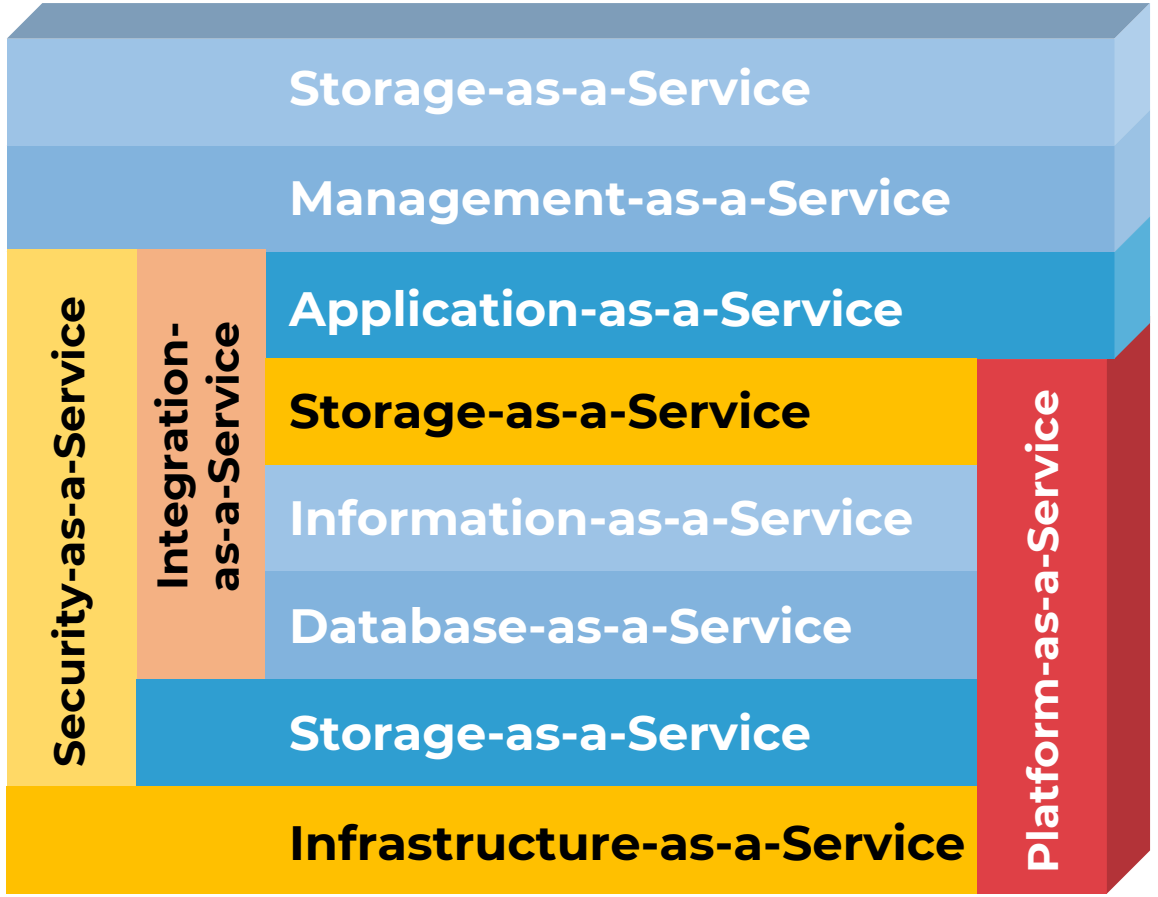
Кто защищает данные в «облаке»

Что такое «облако»:

- ✔ инфраструктура как сервис (Infrastructure as a Service, IaaS);
- ✔ платформа как сервис (Platform as a Service, PaaS);
- ✔ программное обеспечение как сервис (Software as a service, SaaS).

Cloud Computing, 1993 г. Эрик Шмидт

Покупая облако, вы покупаете услуги по обработке персональных данных



https://sonikelf.ru/oblachnye-texnologii-dlya-zemnyx-polzovatelej/

Какие угрозы безопасности таит использование облака

- **Юридическая законность**
  - Соответствие требования по защите ПД
  - Наличие лицензий у поставщика
- **Утечки**
  - Кому принадлежат данные в облаке
  - Кто имеет доступ к данным
- **Утеря данных**
  - Надежность оборудования
  - Архивирование
  - Перестали платить. Что будет дальше?
- **Остановка работы**
  - Обрыв связи
  - Хакерские атаки на сервера владельцев облака
  - Хакерские атаки на клинику

Покупая облако, задавайте вопросы – проверяйте разработчиков

Стоит ли строить слишком высокие заборы

Плюсы

Никто не взломает, никаких утечек и потерь информации

Минусы

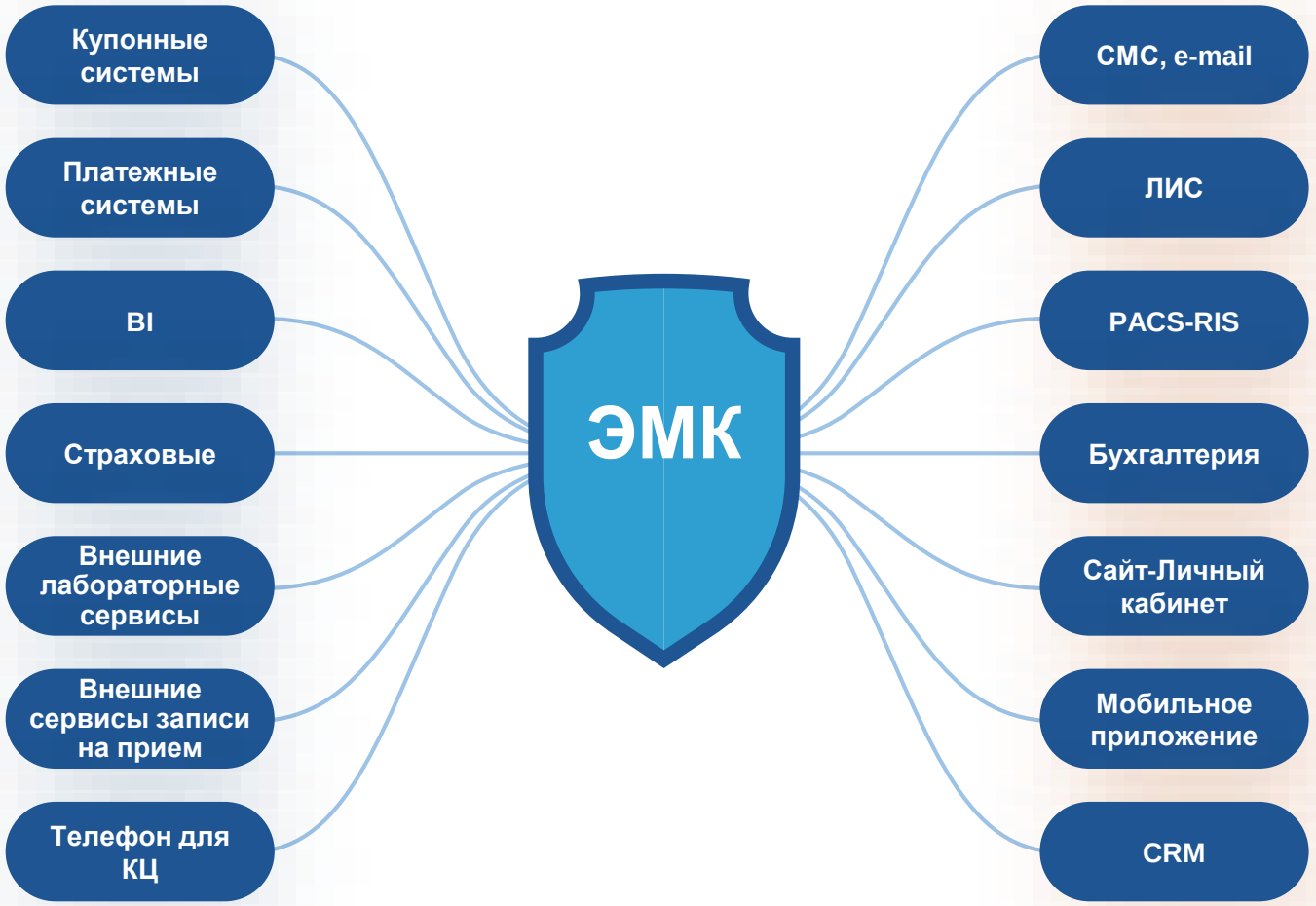
Остановились в развитии. Нет необходимой гибкости в современном быстро меняющемся обществе;

Не могут выстроить современные средства информирования пациентов. Поставщикам услуг затруднен доступ для обслуживания системы, что проявилось в эпоху «удаленки»;

Потеря конкурентоспособности.

Нельзя отказываться от защиты, но и нельзя отгораживаться железным занавесом

Безопасность клиники в работе с внешними сервисами



Риски и угрозы:

- Спам
- Фейковые пациенты
- Утечки будут всегда

Продумывайте авторизацию, читайте договоры

Читаем договор

Пункт договора	Замечание от «Продокторов» («Лицензиат»)
3.7. Лицензиат несет всю ответственность за попытки несанкционированного доступа третьими сторонами к тестовому API или API клиник с использованием учетных данных, полученных Лицензиатом, включая возмещение ущерба пострадавшей стороне.	Исключить данный пункт, т. к. это не находится в ведении Лицензиата.

Комментарии по безопасности

Пункт защищает клинику от утечек пароля.

За защиту и сохранность переданной стороннему разработчику ключевой информации несет ответственность он.

Если произошла утечка и пароли были украдены / скомпрометированы и, с помощью украденных паролей, был нанесен ущерб клинике, за это должен нести ответственность тот, кто не обеспечил сохранность этих данных.

Сложность интеграции с государственными ресурсами

«Для обеспечения безопасности информации в МИС МО ЧСЗ должны применяться средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям безопасности информации.

Информационное взаимодействие МИС МО ЧСЗ с ЕГИСЗ… должно осуществляться с использованием защищенной сети передачи данных.»

Глава 5. Методические рекомендации по организации информационного взаимодействия медицинских информационных систем медицинских организаций частной системы здравоохранения с ЕГИСЗ

https://portal.egisz.rosminzdrav.ru/materials/3639

«Подключение к ЕГИСЗ через клиентские компоненты ViPNet из состава VPN-сети субъекта РФ, работу могут выполнять специализированные компании, обладающие лицензиями ФСБ РФ и ФСТЭК РФ на выполнение данных работ»

Методические рекомендации по защите каналов ЕГИСЗ

https://portal.egisz.rosminzdrav.ru/materials/23

«Испытания проводятся для каждого экземпляра МИС (РМИС), зарегистрированной в ИЭМК согласно заявке на подключение МИС (РМИС) к ИЭМК»

Программа и методика испытаний интеграции с ИЭМК п.3.4.

https://portal.egisz.rosminzdrav.ru/materials/50

Использование цифровой подписи, как защита данных

«2.1. Карта формируется в форме электронного документа, подписанного с использованием усиленной квалифицированной электронной подписи врача, в соответствии с порядком организации системы документооборота в сфере охраны здоровья»

Изменения в приказ в 834н (приказ от 09.01.18 №2н) Порядок заполнения учетной формы N 025/у «Медицинская карта пациента, получающего медицинскую помощь в амбулаторных условиях»

«Процедура подписания ЭПМЗ должна быть активной и осознанной. Медицинский работник должен инициировать процедуру подписания самостоятельно. Компьютерная система не должна навязывать процедуру подписания»

ГОСТ Р 52636-2006. Электронная история болезни

Борисенко Игорь Николаевич

- Инженер-технолог в области разработки и внедрения информационных систем для предприятий
- Эксперт системы менеджмента качества ISO 9001
- Специалист-аналитик по направлению «Аттестация объектов информатизации по требованиям безопасности информации: защита от несанкционированного доступа, защита персональных данных»
- С 1997 года - руководитель направления разработки медицинских информационных систем
- Создатель МИС «ПикоМедицина»
- Генеральный директор ООО «Пикософт», уполномоченный поставщик IT решений Банка России

+7 (495) 660 3818
igor@picosoft.ru