ИТ как фактор доступности, безопасности, качества и эффективности медицинской помощи

Безопасность применения и кибербезопасность медицинских ИТ: нормативные требования, проблемы и решения, практические аспекты

ВЫСШАЯ ШКОЛА УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ
Сеченовский Университет
www.hsha.ru

Столбов Андрей Павлович

Москва, 12 апреля 2018 г.

948.MS.KC

- Глобализация кибератак -> шифровальщики (WannaCry, Petya), блокирование доступа к сервисам, управление IP-камерами *etc* -> поражено более 300 тыс. PC, 120 тыс. камер в 150 странах – 2017
- Рост числа Kill Chain атак -> необходимость мониторинга и оперативной реакции на ИБ-инциденты -> CERT / CSIRT

Взлом и заражение вирусами ЕПГУ (Dr. Web, Kaspersky Lab, июль 2017)

Проникновение в ИС извне (Positive Technologies, 2017)

61% может взломать хакер с "низким потенциалом"
87% не имеют защиты периметра от "пентеста"
98% не были обнаружены действия пентестеров

Утечка конфиденциальной информации (InfoWatch, 2017)

17% из медицинских организаций (48.9% – целевые)
67% через браузер и облачные сервисы / хранилища (в 2016 – 50%)
17% через электронную почту, 8% – бумажные документы

70% инцидентов из-за низкой организации, незнания и халатности !!

- Цифровизация медицинских технологий -> увеличение ИТ-зависимости системы здравоохранения
- Низкая киберзащищенность цифровой медицинской техники
  Нет классификации защищенности медтехники и требований к ее кибербезопасности
- mHealth, "домашняя" телемедицина -> необходимость использовать открытые каналы связи -> высокие риски нарушения конфиденциальности и кибервоздействия на технику
- **Сложность системы защиты и затраты на ИБ стали сопоставимы со сложностью и затратами на решение прикладных задач !!**
- **Более 50% расходов** на ИТ в медорганизациях Европы – **на информационную безопасность** (B. Blobel, октябрь 2016)
- Тенденция дальнейшего роста затрат на ИБ !! : (
- Дефицит специалистов по ИБ – необходимость создания центров компетенции, мониторинга и реагирования на ициденты ИБ

Медицинские ИС как объекты критической информационной инфраструктуры (КИИ)

О безопасности критической информационной инфраструктуры Российской Федерации, закон от 26.07.2017 № 187-ФЗ

> **Объекты КИИ – информационные системы, АСУ, сети связи госорганов, госучреждений, российских юрлиц и предпринимателей (субъектов КИИ), функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, финансов, ТЭК, атомной энергии <...>**

- **Что изменится в работе медицинских организаций ?**
- **Как повлияют новые требования кибербезопасности на рынок медицинских ИТ ?**
- **Как и чем может помочь Минздрав России ?**
- **Что может сделать наше профсообщество ?**
- **Кибербезопасность как осознанная необходимость …**

Правила категорирования и критерии значимости объектов КИИ, постановление Правительства РФ от 08.02.2018 № 127

Правила государственного контроля обеспечения безопасности объектов КИИ, постановление Правительства РФ от 17.02.2018 № 162

Требования к созданию систем безопасности объектов КИИ и обеспечению их функционирования, приказ ФСТЭК от 21.12.2017 № 235

Требования по обеспечению безопасности значимых объектов КИИ, приказ ФСТЭК от 25.12.2017 № 239

Порядок ведения реестра значимых объектов КИИ, приказ ФСТЭК от 06.12.2017 № 227

Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ, приказ ФСТЭК от 11.12.2017 № 229

Проекты приказов ФСБ о Национальном координационном центре – НКЦКИ, предоставлении сведений в ГосСОПКА, информировании ФСБ об инцидентах, обмене информацией об инцидентах, о требованиях к средствам обнаружения, предупреждения и ликвидации последствий компьютерных атак, их установке и эксплуатации

- **Компьютерный инцидент** – факт **нарушения** и(или) прекращения **функционирования** объекта КИИ, сети электросвязи, используемой для взаимодействия таких объектов, и(или) **нарушения безопасности** обрабатываемой информации
- **Категории значимости** объектов КИИ – в зависимости от масштаба возможных негативных последствий в случае возникновения компьютерных инцидентов

  Выявление критических процессов, присвоение категории – критерии

  1. Причинение **ущерба жизни и здоровью** людей (человек), N

     III-я: $1 \leq N \leq 50$; **II-ая:** $50 < N \leq 500$; **I-ая:** $N > 500$ **!?**

  5. Отсутствие доступа к госуслуге – допустимое время, в течение которого госуслуга может быть недоступна (часов), T

     III-я: $12 < T < 24$; **II-ая:** $6 < T < 12$; **I-ая:** $T < 6$

- Утверждение субъектом перечня своих объектов КИИ – **согласование** этого **перечня с Минздравом РФ** (п.15 ПП-127) **?!**

  Максимальный срок категорирования – не более 1 года со дня утверждения субъектом перечня объектов КИИ

- Реестр значимых объектов КИИ – ФСТЭК
- Требования к созданию систем безопасности и обеспечению безопасности объектов КИИ – ФСТЭК
  4 кв. 2018 – единый документ о мерах защиты
- Министерства по согласованию с ФСТЭК могут устанавливать дополнительные требования к защите объектов КИИ с учетом особенностей их сферы деятельности (ст. 11 закона № 187-ФЗ)
  Интегральная модель угроз -> Требования к защите МИС, медтехники, РМИС *etc* !?
- Создание системы защиты объектов КИИ – с учетом требований ПП-1119, приказов ФСТЭК № 21 и № 17 (для ГосИС) + анализ угроз на основе Банка данных угроз ФСТЭК (207 угроз)
- Возможность применения средств защиты информации, прошедших оценку соответствия в форме сертификации или в форме испытаний или приемки (см. закон № 184-ФЗ)
- Выявление уязвимостей, тестирование на проникновение в ИС
- Уведомление об инцидентах – ГосСОПКА, ФСБ

ГОСТ Р 57301-2016 / ISO TS 14441:2013 Требования защиты и конфиденциальности систем EHR (ЭМК), используемые при оценке соответствия (с 01.01.2018)

ГОСТ Р 57640-2017 / ISO/IEC TS 33052:2016 Эталонная модель процесса для управления информационной безопасностью

ГОСТ Р ИСО/МЭК 20933-2017 Распределенные платформы приложений и сервисов (DAPS). Системы доступа

СТО БР ИББС-1.4-2018 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге

ГОСТ Р ИСО 27799-2015 (ISO:2008) Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002

ГОСТ Р 51583-2014 Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования

ГОСТ Р 51624-2000 Автоматизированные системы в защищенном исполнении. Общие положения (ДСП)

Нормативное регулирование обращения медицинского программного обеспечения: практические вопросы

Медицинское изделие – любое изделие, предназначенное для профилактики, диагностики, лечения, реабилитации, мониторинга состояния организма, мед. исследований, не являющееся лекарственным препаратом или биологическим клеточным продуктом [на осн. ст. 38 № 323-ФЗ]

- Какое ПО относится к медицинским изделиям (МИ)

  Software as a Medical Device (SaMD) – программное медизделие

  Самостоятельное ПО – класс риска – как для **активного** МИ

- Основные этапы процедуры госрегистрации ПО как МИ

  Испытательные лаборатории (их 10, см. www.roszdravnadzor.ru)

- Требования к документации на ПО, отнесенное к медицинским изделиям – приказ Минздрава РФ от 19.01.2017 № 11н

Ответственность за нарушения в сфере обращения медицинских изделий – ст. 6.28, 6.33, 19.5, 19.7.8 КоАП РФ, ст. 238.1 УК РФ

Номенклатурная классификация медицинских изделий

приказ Минздрава РФ № 4н от 06.06.2012 в ред. пр. № 557н от 25.09.2014

- по **видам** – в зависимости от назначения, особенностей конструкции и устройства – **www.roszdravnadzor.ru/services/mi_reesetr**

  Код вида МИ (**только один**) – в РУ, для поиска в реестре МИ, указания в стандартах оказания медпомощи *etc*
- по **классам** потенциального **риска** применения (1, 2а, 2б, 3)

  Риск применения МИ – риск, который **нельзя снизить** организационными и техническими мерами.

  Надо ли при определении класса риска применения МТ учитывать риски, связанные с кибербезопасностью**?**

Критерии отнесения ПО к МИ -> для **подтверждения** безопасности и эффективности применения МИ нужны **клинические данные** **!!**

Клинические испытания МИ в форме – для:

класса 1 (низкий риск) – **анализа и оценки** клинических данных

других классов – **контролируемых** клинических испытаний

Письмо Росздравнадзора от 30.12.2015 № 01И-2358/15:

программное обеспечение является медицинским изделием и полежит госрегистрации если оно предназначено для:

- **мониторинга, управления работой медтехники (МТ)**
- **получения от МТ диагностических данных, их накопления и расчета? в автоматическом режиме**
- **мониторинга функций организма человека и передачи полученных данных (в т.ч. по беспроводным каналам)**
- **расчета параметров подбора дозы (облучения, лекарственного средства, контрастного вещества и т.д.)**
- **обработки данных, полученных с диагностического медицинского оборудования, передачи их на системы планирования? и терапии**
- **обработки медицинских изображений**
- **3D-моделирования**
- **связи диагностического и лечебного оборудования**

Если ПО включено в Номенклатуру видов МИ, но не предназначено для выполнения этих функций, то оно не является МИ ?!

= клинически важные / значимые функции обработки данных

1) Относится ли к медицинским изделиям ПО, если по своему назначению и характеристикам оно соответствует какой-либо категории ПО, включенной в Номенклатуру видов МИ?

2) Как определить вид МИ для ПО, если по номенклатуре оно может быть отнесено к нескольким (разным) видам?

Назначение "модуля" -> вид -> как отдельное МИ -> свое РУ

3) Надо ли регистрировать "медицинское" ПО, указанное в письме от 30.12.2015, введенное в эксплуатацию до 06.01.2015? -> ДА !!

4) Надо ли регистрировать "самописное" ПО, если оно применяется в МО только для собственных нужд?

5) В каких случаях организации-разработчику "медицинского" ПО надо получать лицензию на осуществление деятельности по производству и техническому обслуживанию медтехники?

6) Кто и как сможет проверить наличие и использование незарегистрированного медицинского ПО?

Приказы Росздравнадзора от 20.12.2017 № 10449, № 10450 – контрольные листы

Медицинские ИТ: импортозамещение, особенности государственных закупок

- Реестр российского программного обеспечения. Требования нормативных документов

  Постановление Правительства РФ от 16.11.2016 № 1236 (ред. от 07.03.2018) -> реестр российского ПО – Минкомсвязи РФ, https://reestr.minsvyaz.ru/reestr/
- Особенности поставки ПО и ИТ-сервисов, предназначенных для автоматизации медицинской деятельности
- Лицензии, которые необходимо иметь разработчикам и поставщикам указанного ПО и ИТ-сервисов
- Типичные ошибки при проведении государственных закупок ИТ-продукции для медицинских учреждений

Наличие лицензий ФСТЭК и ФСБ* у поставщиков услуг или средств

- по контролю защищенности ИС (пентесты), мониторингу информационной безопасности
- по аттестации объектов автоматизации (по требованиям ИБ)
- по **проектированию ИС в защищенном исполнении**
- по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации
- криптографической защиты информации* (в т.ч. создание, продажа)

Наличие аттестата соответствия ЦОД, в котором обрабатываются персональные данные, требованиям ИБ

Наличие лицензий ФСТЭК у разработчика ПО при реализации в МИС собственных функций защиты информации (системы управления доступом *etc*) [письмо ФСТЭК от 08.06.2017 № 240/13/2793]

Наличие лицензии Росздравнадзора на производство и техобслуживание медтехники – при поставке и сопровождении ПО, зарегистрированного как медизделие – для ЛИС, РИС *etc*

Право заказчика указать в ТЗ на ИС (ИТ-сервис?) требования о наличии сертификатов соответствия требованиям ИБ, на средства защиты *etc*

Некоторые типичные ошибки при госзакупках ИТ-продукции

- неверное определение объекта закупки, чаще всего – при оказании "облачных" услуг (вместо IaaS – SaaS *etc*)
- отсутствие требований к поставщику, предусмотренных законодательством (наличие лицензий, аттестата ИБ на ЦОД etc)
  [ст. 32, 33 закона № 44-ФЗ]
- отсутствие ссылок на ГОСТы при описании объекта закупки
  [п.2 ч.1 ст.34 закона № 44-ФЗ]
- отсутствие требований о наличии у поставщика прав на объекты интеллектуальной собственности
  [п.8 ч.1 ст.31, п.1 ч.1 ст.33 закона № 44-ФЗ]
- отсутствие требований к составу и содержанию документов при передаче исключительных прав на заказное ПО
- нечеткое указание порядка приема работы, услуги и критериев качества [ст.34 закона № 44-ФЗ]
- отсутствие перечня возможных мероприятий по переносу ПО и портированию БД на ресурсы ЦОД, указанного заказчиком; невключение затрат в НМЦК

Предложения

- Формализовать и утвердить критерии отнесения ПО к МИ. Разработать методрекомендации по регистрации ПМИ. Исключить из Номенклатуры видов МИ ПО, предназначенное для выполнения административных и учетных функций, ведения мед. документации, формирования статотчетов, управления ресурсами
- Разработать типовую отраслевую интегральную модель угроз информационной безопасности (медтехника, МИС, персданные) + комплект нормативных и методических документов по обеспечению кибербезопасности в здравоохранении
- Разработать практические рекомендации (типичные кейсы), предусмотреть в "дорожных картах" мероприятия по повышению осведомленности специалистов и руководителей в вопросах ИБ, госзакупок ИТ-продукции *etc*

Нужны конкретные рекомендации со стороны авторитетного независимого органа – ЦНИИОИЗ, АРМИТ, НАМИ, лучше – в виде совместных документов, исходящих из Минздрава России

Благодарю за внимание, вопросы и дискуссию!

Столбов Андрей Павлович

ap100Lbov@mail.ru

www.hsha.ru

Вестник Росздравнадзора, 2017, № 3 (классы риска для ПО)
Проблемы стандартизации в здравоохранении, 2017, № 3-4

Сеченовский Университет

ВЫСШАЯ ШКОЛА УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ

"Облачные" технологии обработки данных / сервисы – доступ пользователей к информационным и вычислительным ресурсам удаленного центра обработки данных (ЦОД) через телекоммуникационную сеть с помощью web-браузера

Web-браузер – компьютерная программа для доступа и работы с сайтами в Интернет, с локальными или "облачными" приложениями, реализованными по стандартам Интернет (web)

IaaS – Infrastructure as a Service – аренда оборудования, системного ПО и средств защиты информации ЦОДа – прикладное ПО устанавливает сам пользователь !!

SaaS – Software as a Service – использование установленного в ЦОД прикладного ПО (принадлежит провайдеру)

DDaaS – Data Depository as a Service – "облачное" хранилище данных

Данные (базы данных) во всех случаях храняться в ЦОД !!

Оператор (провайдер) канала передачи данных / VPN !?

Использование "облачных" ИС – логистика и риски

- **Невозможность полного контроля** процессов обработки данных и доступа к данным -> **доверие** к поставщику "облачных" сервисов -> **сертификация ПО, аттестация поставщика, ЦОД *etc* по требованиям информационной безопасности !?**
- **Зависимость от надежности и защищенности канала** передачи данных -> риски блокирования доступа к "облачным" сервисам -> доверие к оператору канала -> **сертификация, аттестация *etc***
- Проблемы при **смене поставщика** сервисов -> необходимость переноса баз данных – нужны мощности, время, ресурсы *etc*
- Периодическое резервное копирование баз данных (БД) на технические средства пользователя (архивирование данных)
- Необходимость стандартизации и технологической нейтральности форматов представления записей для выгрузки / загрузки информации из БД
- Проблемы с подключением медицинской техники к "облачным" ЛИС, РИС *etc* – только асинхронный (OFF-Line) режим (ЦАМИ)

Отнесение ПО к медицинским изделиям ->

- **обязательная оценка соответствия, экспертиза качества, эффективности и безопасности** – технические испытания и клинические испытания (приказы Минздрава РФ от 09.01.2014 № 2н, от 06.06.2012 № 4н (ред. от 25.09.2014), от 15.08.2012 № 89н, от 21.12.2012 № 1353н (ред. от 03.06.2015), от 19.01.2017 № 11н)
- **государственная регистрация**, включение в госреестр медицинских изделий и организаций, осуществляющих их производство и изготовление (постановление Правительства России от 27.12.2012 № 1416) -> регистрационное удостоверение
- **мониторинг безопасности** медицинских изделий (постановление Правительства РФ 25.09.2012 № 967, приказ Минздрава РФ от 14.09.2012 № 175н)

Требования к содержанию технической и эксплуатационной документации производителя (изготовителя) медицинского изделия (приказ Минздрава РФ от 19.01.2017 № 11н)

ГОСТ Р ИСО/ТС 25238-2009 / ISO/TS:2007 Классификация угроз безопасности от медицинского программного обеспечения (ПО)
ГОСТ Р ИСО/ТО 27809-2009 / ISO/TR:2007 Меры по обеспечению безопасности пациента при использовании медицинского ПО
ГОСТ Р МЭК 62304-2013 / IEC:2006 Изделия медицинские. Программное обеспечение. Процессы жизненного цикла*
ГОСТ Р МЭК 62366-2013 / IEC:2006 Проектирование медицинских изделий с учетом эксплуатационной пригодности* [юзабилити]
ГОСТ Р 56849-2015 / ISO/TR 17791:2013 Руководство по стандартам безопасности медицинского ПО
ГОСТ Р 56429-2015 Изделия медицинские. Клиническая оценка

IMDRF/SaMD WG/N10:2013 Software as a Medical Device: Key Definitions
IMDRF/SaMD WG/N12:2014 Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations
IMDRF/SaMD WG/N23:2015 Software as a Medical Device: Application of Quality Management System
IMDRF/SaMD WG/N41:2017 Software as a Medical Device: Clinical Evaluation, принят 21.09. 2017

Потенциальный риск применения МИ – комбинация вероятности причинения вреда при применении МИ в соответствии с его назначением, и тяжести этого вреда

Вред – травмирование или наненсение ущерба здоровью человека, оборудованию или окружающей среде

Опасность (угроза) – потенциальный источник вреда

Опасная ситуация – обстоятельства, при которых люди, имущество или окружающая среда подвержены одной или нескольким опасностям (угрозы -> опасная ситуация)

Вероятность причинения вреда – произведение (суперпозиция) вероятностей возникновения опасностей и возниконовения опасной ситуации

Класс риска МИ -> **требования** к процессам и процедурам на всех этапах жизненного цикла МИ (разработка, испытания – оценка качества, эффективности и безопасности – производство, регистрация, применение, сопровождение, мониторинг безопасности) -> **разумная достаточность !!** -> **сокращение** общественных **издержек**

Принадлежности – предметы, самостоятельно не являющиеся МИ и по целевому назначению применяемые совместно с МИ либо в их составе для того, чтобы МИ могло быть использовано в соответствии с назначением

Вид медицинского изделия – определенная обобщающая категория для некоторой совокупности медицинских изделий, имеющих аналогичное либо схожее назначение и/или устройство -> **код + наименование** вида **+ описание** вида

Регистрация МИ -> наименование, сведения о производителе +

- назначение МИ, определенное производителем
- отнесение к определенному **виду** МИ – только к одному **!!**
- определение **класса риска** применения
- состав изделия, принадлежности
- указание сведений о взаимозаменяемых изделиях

Номенклатурная классификация по видам -> поиск в государственном реестре МИ, идентификация МИ в стандартах медицинской помощи

Соглашение о единых принципах и правилах обращения медицинских изделий в рамках ЕАЭС (*закон № 4-ФЗ от 31.01.2016*)

- единые правила в соответствии с рекомендациями Международного форума регуляторов медицинских изделий (IMDRF, www.imdrf.org)
- гармонизации номенклатуры медицинских изделий (МИ) с Global Medical Device Nomenclature (GMDN, www.gmdnagency.org)
- единая информационная система ЕАЭС в сфере обращения МИ

Решения ЕАЭС – вступили в силу в мае 2017, переход до 31.12.2021

- **№ 17** перечень стандартов от 04.09.2017
- **№ 27** требования безопасности и эффективности МИ
- **№ 28** правила технических испытаний МИ
- **№ 29** правила клинических и клинико-лабораторных испытаний МИ
- **№ 49** правила регистрации и экспертизы безопасности, качества и эффективности МИ
- **№ 106** требования к системе менеджмента качества МИ
- **№ 173** классификация в зависимости от риска применения МИ
- **№ 174** порядок мониторинга безопасности МИ
- **№ 177** номенклатура медицинских изделий

Самостоятельное ПО = SaMD

Врач (ЛВ) – Врач (ВК), открытый канал связи (ОКС), АР

-> шифрование ЭД

Установка СКЗИ на РС ЛВ и ВК + Инфраструктура ключей (PKI)

-> псевдонимизация ЭД -> установка ПО-П только на РС ЛВ !!

Врач – Врач, открытый канал связи, ВКС

-> без показа лица и упоминания ФИО пациента (обезличенно)

(Пациент + МИ) – Врач, открытый канал связи, телемониторинг

Привязка ($ID_{МИ}$: ПДн пациента) на РС врача -> персданные по открытому каналу не передаются (так же МИ -> Пациент -> Врач)

Согласие на телемониторинг, на ТМУ (ст. 20 № 323-ФЗ) ?!

Пациент – Врач, открытый канал связи, АР, ВКС -> защита ?!

-> согласие пациента на передачу данных по ОКС

Информированное согласие (ст. 9, № 152-ФЗ) -> предупредить о риске нарушения конфиденциальности (ст. 18.1 № 152-ФЗ)

-> организация временного защищенного канала (VPN)

Применение LPS- или аналогичных устройств на РС пользователей Lightweight Portable Security, см. http://spi.dod.mil

Проблемы обмена данными по открытым каналам связи

HTTPS -> проблема достоверной аутентификации источника

Man-In-The-Middle, Man-In-The-Browser – потенциал нарушителя !?

Взлом ЕПГУ (Dr. Web, Kaspersky Lab)

Рассылка писем с вирусом от имени ЕПГУ, февраль 2015

Заражен вирусом, 13.07.2017 -> проблема устранена 14.07.2017

Возможные решения

- строгая аутентификация с использованием аппаратных средств (устройств типа eToken, SIMiD *etc*)
- применение LPS-устройств (Lightweight Portable Security) на основе LiveUSB – создание защищенного АРМ, шифрование, VPN-клиенты, работа с Э-документами (ключи ЭП) *etc* (см. Sofware Protection Initiative, http://spi.dod.mil)

Обязательная сертификация средств шифрования для передачи в сети Интернет сведений, не составляющих гостайну, **не требуется !!**

ФСБ, 18.07.2017, www.fsb.ru

Письмо ФСТЭК от 08.06.2017 № 240/13/2793 (повтор письма от 20.06.2016 № 240/13/2754) – при наличии / реализации в МИС собственных функций защиты информации, например, системы управления доступом, разработчику ПО нужна лицензия:

- на разработку средств технической защиты информации (ТЗИ)
- на техническое обслуживание средств ТЗИ

Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения, **приказ Роскомнадзора от 30.05.2017 № 94**

Рекомендации Роскомнадзора от 31.07.2017 по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном законом от 27.07.2006 № 152-ФЗ "О персональных данных"

[http://rkn.gov.ru/docs/Rekomendacii31072017.docx]

Банк данных угроз безопасности информации (БДУ) ФСТЭК

– www.bdu.fstec.ru, сообщение ФСТЭК от 06.03.2015 № 240/22/879

ГосНИИИ ПТЗИ ФСТЭК России

Угроз – **207**, уязвимостей – **18356** (на 06.04.2018)

★ При создании системы защиты информации должно быть подтверждено, что в ГосИС отсутствуют уязвимости, содержащиеся в БДУ (приказ ФСТЭК № 17, пп. 14.3, 16.6) **!!!**

Калькуляторы для оценки уязвимостей – CVSS v.2.0, v.3.0
Common Vulnerability Scoring System, www.first.org/cvss-guide.html

---

- Common Vulnerabilities and Exposures (CVE), http://cve.mitre.org
- National Vulnerabilities Database (NVD), http://nvd.nist.gov
- Vulnerability Notes Database (VND), http://www.us-cert.gov
- Open Source Vulnerabilities DataBase (OSVDB)*), http://osvdb.org

*) с 08.04.2016 ведется в режиме блога

Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных ИС,
постановление Правительства РФ № 676 от 06.07.2015 в ред. от 11.05.2017 № 555

- при создании, развитии, эксплуатации <...> государственных ИС должны выполняться требования по защите информации, устанавливаемые ФСБ и ФСТЭК
- предусмотрен **новый этап** – формирование требований по защите информации и к организации и мерам защиты – на основе модели угроз безопасности информации; модель угроз, требования к защите, ТЗ на создание ГосИС согласуются с ФСБ и ФСТЭК
- не допускается ввод в эксплуатацию без аттестации ГосИС на соответствие требованиям защиты информации
- развитие / модернизация ГосИС осуществляется в соответствии с установленными требованиями по защите информации

Обязательная сертификация средств шифрования для передачи в сети Интернет сведений, не составляющих гостайну, **не требуется – ФСБ, 18.07.2017, www.fsb.ru !!**

ГОСТ Р 51583, 51624, 56939 – ИС в защищенном исполнении

ГОСТ Р ИСО/МЭК 27002-2012 Свод норм и правил менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27003-2012 Руководство по реализации системы менеджмента информационной безопасности.

ГОСТ Р ИСО 27799-2015 Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002

ГОСТ Р 56849-2015 / ISO/TR 17791:2013 Руководство по стандартам безопасности медицинского программного обеспечения

ГОСТ Р МЭК 80001-1-2015, ГОСТ Р 56839, 56850, 56840, 56841-2015 Менеджмент рисков в информационно-вычислительных сетях с медицинскими приборами (IEC/TR 80001-2-1, 2-2, 2-3, 2-4:2012)

ГОСТ Р 56837, 56838-2015 / ISO/TR 11633-1:2009 Менеджмент информационной безопасности удаленного технического обслуживания медицинских приборов и медицинских ИС

Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов РФ, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют **угрозы безопасности персональных данных, актуальные при их обработке в ИС, эксплуатируемых при осуществлении соответствующих видов деятельности**, с учетом содержания персональных данных, характера и способов их обработки

=> **отраслевая модель (перечень) угроз безопасности персональных данных -> Минздрав РФ, ФОМС, ФСС**

[*часть 5 ст. 19 закона № 152-ФЗ*]

Новый комплект нормативно-методических документов по ИБ для организаций здравоохранения и ОМС **!?**

Перечень услуг, предоставляемых через ЕПГУ – с 01.01.2018

распоряжение Правительства РФ от 15.11.2017 № 2521-р

Медицинские организации

Реестр госуслуг, предоставляемых в электронной форме – № 1526-р от 19.07.2017

- запись на прием к врачу
- прием заявки на вызов врача на дом
- предоставление доступа? к медицинским документам
- предоставление сведений о прикреплении к медицинской организации
- запись на прохождение проф. медосмотров / диспансеризации

Территориальные фонды ОМС

Сведения из/в ТФОМС – № 2183-р от 06.10.2017

- предоставление застрахованному лицу информации о перечне оказанных ему мед. услуг и их стоимости за указанный период
- подача заявления о выборе СМО

Минздрав России

- предоставление сведений об оказанной медицинской помощи, содержащихся в ЭМК
- предоставление сведений о полисе ОМС и СМО

Оценка качества работы МО через ЕПГУ (эксперимент 01.04-31.12.2018),

постановление Правительства РФ от 06.03.2018 № 230

ГОСТ Р 55349-2012 Форматы описания и нормирования требований (ФОНТ). Руководство по разработке и применению

ГОСТ Р 55353-2012 ФОНТ. Система информации о показателях и требованиях к производственному менеджменту

ГОСТ Р 55354-2012 ФОНТ. Система информации о показателях и требованиях к менеджменту рисков

ГОСТ Р 55357-2012 ФОНТ. Система информации о показателях и требованиях к медицинской технике

ГОСТ Р 55359-2012 ФОНТ. Система информации о показателях и требованиях к системам контроля и мониторинга

ГОСТ Р 55351-2012 ФОНТ. Система информации о показателях и требованиях к компетентности экспертов и экспертных организаций

ГОСТ Р 56262-2014 Надлежащая практика регулирования. Руководство по оценке эквивалентности требований