MedSoft – 2017

Non nocere!

Безопасность медицинских информационных технологий: новые задачи, старые проблемы

ВЫСШАЯ ШКОЛА УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ

www.hsha.ru

Столбов Андрей Павлович

Москва, 13 апреля 2017 г.

12.4.7 КС

Есть здравый смысл.

Есть реальная практика … и …

Есть нормативные требования …

Dura lex, sed lex!

Non nocere !!!

Проблема надежной аутентификации -> eID, BioID, Digital Signature, федеративные системы аутентификации !!

ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity

Киберпреступность

Угрозы нарушения
- **конфиденциальности**
- **целостности**
- **доступности информации**

Угрозы раскрытия / выявления параметров системы защиты / защищенной АС

Борьба с DoS-атаками!!

Переход на гарвардскую архитектуру?

Безопасность работы в киберпространстве
- **способность противостоять внешним и внутренним угрозам и воздействиям**
- **работа АС не создает угроз ИБ для внешней среды (внешних сетей и АС)**

Проблемы аутентификации!!

Кибербезопасность – это постоянный процесс !!

PDCA: Plan – Do – Check – Act & OODA: Observe – Orient – Decide – Act

Dr. Google -> доверие к Интернет-сайтам !?

COM(2002) 667, eEurope 2002: Quality Criteria for Health related websites + Health On Net Foundation, www.hon.ch !!

57% приходят к врачу со "своим диагнозом"

35% просят выписать определенное лекарство

49% занимаются самолечением "из Интернет"

Rock Health, 2015

Если вы лечитесь по медицинскому справочнику, то рискуете умереть от опечатки … : (

16% врачей ищут информацию о своих пациентах в Интернет (Австралия, США, Канада)

Univadis, 10 апреля 2017

Интернет – это всемирная информационная "помойка" !!

Гарантированно защитить и удалить данные (в)из Интернет невозможно !!

Кибербезопасность – фактор доступности, безопасности и качества медицинской помощи

- Широкое применение компьютеров и Интернет в медицинской практике, науке и образовании
- "Цифровизация" медицинских технологий
  Digital Medical Device + Software as a Medical Device (SaMD)
- Рост количества атак на компьютерные системы, интенсивная разработка и применение новых способов кибервоздействия

315 тысяч новых вирусов в день в 2015 (Kaspersky_Lab, 2016)

100% ежегодный рост числа DDoS-атак в РФ (Qrator_Labs, 2016)

750% рост числа атак "шифровальщиками" за 2016 (Trend Micro)

DICOM-серверы в открытом доступе: США – **24%**, РФ – **44%**

www.auntminnie.com, 2016

- **отказ** медицинской техники: КТ, МРТ, УЗИ, анализаторов в КДЛ, кардиостимуляторов, инсулиновых помп *etc*
- **утечка** персональных и коммерческих данных *etc*
- **удаление, искажение, блокирование** доступа к данным, ЭМК *etc*

Безопасность применения ИТ здравоохранении

- **Информационная (кибер)безопасность** (ИБ, КБ) -> защита:
  - персональных данных и врачебной тайны (ИС ПДн)
  - МИС (SaMD *etc*) и электронных документов (ЭМК)
  - медицинской техники (МТ) -> класс защищенности **?!**

    Требования к защищенности ИС МО в целом **?**

    Интегральная модель угроз: ПДн - МИС - ЭДО - МТ *etc* **!!**

- **Безопасность применения** медицинских ИТ для жизни и здоровья пациента и персонала -> "клинический" риск при использовании ИТ как элемента медицинской технологии:
  - цифровой медицинской техники -> класс риска
  - программных медицинских изделий (SaMD) -> класс риска
  - первичных электронных медицинских документов (ЭМК) **!?**
  - медицинских Интернет-ресурсов для врачей и пациентов

Документ -> юридическая значимость -> электронная подпись

Доверие врача и пациента к медицинским ИТ ->
подтверждение безопасности, качества и эффективности ->
валидация !! -> идентификация и оценка рисков ->
испытания -> сертификация -> государственная регистрация
-> государственный контроль и надзор + мониторинг
безопасности применения *etc*
+ лицензирование – аттестация – аккредитация

Кибербезопасность – составная часть безопасности медицинской деятельности **!!**

В чем специфика обеспечения кибербезопасности в здравоохранении, в том числе при обработке персональных данных и обмене электронными медицинскими документами **?**

Кто регулирует, контролирует и надзирает **?**

Нормативное регулирование в сфере обеспечения безопасности применения ИТ в здравоохранении !!

NIST Cybersecurity Framework (CSF, февраль 2014 -> июль 2015)

DHHS Office for Civil Rights: HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework (февраль 2016)

FDA: руководства по мониторингу инцидентов КБ (2013), обеспечению КБ медизделий на этапе разработки и производства (2014), в процессе эксплуатации (проект, янв. 2016) – **классификация медизделий -> состав мер и "контролей" КБ**

Обязательная сертификация "медицинского" ПО в США:

в ONC – интероперабельность и ИБ (HIPAA-HITECH, 2009)

в FDA – безопасность для пациента (как медизделие)

HITRUST – центр компетенции и CERT -> CSF for Health care

www.hitrustalliance.net

в **57%** клиник США есть специалисты по кибербезопасности

Ponemon Institute, май 2016

42 успешные атаки на медтехнику и МИС в 2015 – **16%** успешных атак во всех отраслях в США (US-CERT, HITRUST, май 2016)

NIS Directive EU 2016/1148 -> CSIRT, тестирование ИС всех клиник

Указы Президента Российской Федерации

О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена, № 351 от 17.03.2008

О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, № 31с от 15.01.2013

Стратегия национальной безопасности РФ, № 683 от 31.12.2015

Доктрина информационной безопасности РФ, № 546 от 05.12.2016

Профилактика – Диагностика – Лечение – Реабилитация

ГосСОПКА -> Национальный центр по компьютерным инцидентам (ФСБ России)

FinCERT – Центробанк России, www.cbr.ru

Проблемы сокрытия инцидентов ИБ !!

Требования к антитеррористической защищенности объектов, относящихся к сфере деятельности Минздрава России, постановление Правительства РФ **от 13.01.2017 № 8**

в том числе фонды ОМС, СМО, аптеки *etc*

16. В целях обеспечения необходимой степени антитеррористической защищенности объектов (территорий) независимо от присвоенной им категории осуществляются следующие мероприятия:

а) организация и обеспечение пропускного и внутриобъектового режимов на объекте (территории), контроль их функционирования;

<...>

е) организация обеспечения информационной безопасности, разработка и реализация мер, исключающих несанкционированный доступ к информационным ресурсам объекта (территории);

<...>

л) поддержание в исправном состоянии инженерно-технических средств и систем охраны, оснащение бесперебойной и устойчивой связью объекта (территории);

Проект федерального закона № 47571-7 о безопасности критической информационной инфраструктуры (КИИ) РФ

- объекты КИИ – ИС и сети связи госорганов, а также АСУ ТП, функционирующие в оборонной промышленности, в области здравоохранения, транспорта, связи, энергетики, финансов <...>
- объекты КИИ проходят категорирование на основании критериев, утверждаемых Правительством РФ
- создание государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ –> ГосСОПКА
- федеральный орган, уполномоченный в области обеспечения безопасности КИИ устанавливает требования к средствам ГосСОПКИ и системам защиты на объектах КИИ
- министерства по согласованию с указанным выше органом могут устанавливать дополнительные требования к защите объектов КИИ исходя из особенностей их функционирования
- создание системы защиты инфорации на объектах КИИ

Проект федерального закона № 52657-7 (изм. в № 149-ФЗ)

- операторы государственных ИС и **иных ИС, в которых обрабатывается информация, обладателями которых являются государственные органы***), создают системы защиты информации в указанных ИС
- требования к защите информации в государственных и иных ИС, в которых обрабатывается информация, обладателями которой являются госорганы, устанавливаются ФСБ и ФСТЭК
- обязанность операторов указанных выше ИС информировать уполномоченные органы власти о компьютерных инцидентах, в результате которых нарушены функционирование ИС и/или ИБ

---

*) **пользователи и/или поставщики информации, аутсорсеры ?!**

Аутсорсинг обработки даных -> невозможность контроля средств и процесса обработки со стороны пользователя (заказчика) -> **доверие** -> **лицензирование, аккредитация, аттестация ?!**

Проект изменений в Требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных ИС

утв. постановлением Правительства РФ № 676 от 06.07.2015

- при создании, развитии, эксплуатации <...> государственных ИС должны выполняться требования по защите информации, устанавливаемые ФСБ и ФСТЭК
- предусмотрен новый этап при создании ГИС – формирование требований по защите информации
- модель угроз безопасности информации и требования к защите ГИС утверждаются руководителем оператора
- создание ГИС осуществляется в соответствии с ТЗ, согласованным в части, касающихся требований по защите информации с ФСБ и ФСТЭК -> создание АС в защищенном исполнении (ГОСТ Р 51583) !!?
- не допускается ввод в эксплуатацию без аттестации ГИС на соответствие требованиям защиты информации

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 – 194, уязвимостей – 15987 (на 10.04.2017)

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

Калькулятор для оценки уязвимостей – CVSS v. 2.0
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 о защите информации, не составляющей гостайну, содержащейся в государственных ИС (приказ ФСТЭК от 11.02.2013 № 17, в ред. приказа № 27 от 15.02.2017) !!

- три класса защищенности ГИС: К1 > К2 > К3 (было 4)
- определение угроз безопасности информации, потенциала нарушителя и анализ уязвимостей на основе **БДУ ФСТЭК !!**
- учет потенциала нарушителя при определении состава организационных мер и СрЗИ: высокий потенциал*) -> К1, не ниже усиленного базового*) -> К2, не ниже базового*) -> К3
- изменено соотнесение классов применяемых ОС, средств защиты информации (СрЗИ) с классами ГИС
- расширены состав мер защиты и видов аттестационных испытаний

---

*) потенциал нарушителя – классификация ?!

Меры защиты информации в государственных информационных системах. Методический документ. Утвержден ФСТЭК 11.02.2014 ?!

ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования (*с 01.06.2017*)

ГОСТ Р 56938-2016 Защита информации при использовании технологий виртуализации. Общие положения (*с 01.06.2017*)

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

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

ГОСТ Р ИСО/МЭК 27034-1-2014 Информационные технологии. Безопасность приложений. Часть 1. Обзор и общие понятия

ГОСТ Р 56545, 56546-2015 Уязвимости информационных систем. Правила описания уязвимостей. Классификация уязвимостей

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

ГОСТ Р 56875-2016 Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий

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

ГОСТ Р ИСО 17090-4-2016 Электронные подписи медицинских документов

ГОСТ Р ИСО 27789-2016 Журналы аудита для электронных медицинских карт

ГОСТ Р ИСО 27799-2015 (2008) Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002 (с 01.11.2016) !!

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

ГОСТ Р ИСО 17090-1, -2, -3-2015/16 Информатизация здоровья. Аутентификация на основе цифровых сертификатов

ГОСТ Р ИСО/ТС 22600-1, -2-2009, -3-2013 Информатизация здоровья. Управление полномочиями и контроль доступа

ГОСТ Р 54472-2011 / ISO/TS 13606-4:2009 Передача электронных медицинских карт. Часть 4 Безопасность

ГОСТ Р ИСО 13119-2016 Источники клинических знаний. Метаданные -> уровни доверия, доказательности *etc*

ГОСТ Р ИСО 14199-2016 Информационные модели. Модель интегрированной предметной области биомедицинских исследований (BRIDG – Biomedical Research Integrated Domain Group, CDISC, www.cdisc.org)

ГОСТ Р 56848-2015 / ISO/TR 13054-1:2012 Менеджмент знаний стандартов информатизации здоровья (с 01.11.2016)

ГОСТ Р 56044-2014 Оценка медицинских технологий. Общие положения

ГОСТ Р 57377-2016 / ISO/TR 16056-2:2004 Функциональная совместимость систем и сетей телездравоохранения. Часть 2. Системы реального времени

Обезличивание персональных данных

- **необратимое** -> обратная **персонификация невозможна**
- **обратимое** -> присвоение **псевдонима**

ГОСТ Р 55036-2012 / ISO/TS 25237:2008 Информатизация здоровья. Псевдонимизация (**ISO 25237:2017**)

ГОСТ Р ИСО/ МЭК 27038-2016 (ISO:2014) Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования (с 01.07.2017)

Требования и методы по обезличиванию персональных данных, приказ Роскомнадзора № 996 от 05.09.2013 г.

Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 г. № 996, утверждены 13.12.2013 г.

Обезличенные данные уже **не являются персональными** данными -> другие требования к их защите и доступу ("нет тайны") **!!**

Примененение технологий псевдонимизации

– вторичное использование полицевых медицинских данных

- ведение медицинских регистров – нозологических, геномных (ДНК), генетических, потенциальных доноров органов и тканей, в психиатрии *etc* ("Декларация Монтре", сентябрь 2005 г.)
- при проведении клинических исследований и испытаний -> ГОСТ Р ИСО 14155-2014 Клинические исследования
- база данных интегрированных электронных медицинских карт граждан (ИЭМК: интегральный анамнез жизни, эпикризы *etc*)

база данных выписных эпикризов Spine в Англии

Согласие пациента на обработку псевдонимизированных данных с учетом риска компрометации псевдонима ?!

Практика -> соглашение: правила псевдонимизации и обратной персонификации медицинских документов

- централизованные клинические лаборатории
- телерадиология, дистанционная расшифровка ЭКГ *etc*
- "второе мнение" по документам *etc*

Постановления Правительства РФ

Правила организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, **организациях с государственным участием** и организациях оборонно-промышленного комплекса (№ 399 от 06.05.2016)

Положение о лицензировании деятельности по технической защите конфиденциальной информации (№ 79 от 03.02.2012 в ред. от 15.06.2016) – **с 01.06.2017 наличие лицензии** при оказании услуг:

- по **контролю защищенности** от утечек по техническим каналам и несанкционированного доступа к информации (пентесты *etc*)
- по **мониторингу** информационной безопасности
- по **аттестации** объектов автоматизации
- по **проектированию в защищенном исполнении**
- по **установке,** монтажу, наладке, испытаниям, **ремонту средств защиты информации**

Унификация и комплексирование средств защиты информации со средствами квалифицированной электронной подписи и VPN + прикладное ПО + базы данных -> доступ в личный кабинет, персональный носитель медицинских данных, ТМ *etc* ->

Технология LPS (*Lightweight Portable Security*) на основе LiveUSB для создания VPN-клиентов, защищенных АРМ, работы с электронными документами -> сертификация, тиражирование

Sofware Protection Initiative, http://spi.dod.mil

Профессиональные стандарты, осень 2016 -> специалист по:

- защите информации в автоматизированных системах
- технической защите информации
- безопасности компьютерных систем и сетей
- защите информации в телекоммуникационных системах и сетях
- автоматизации информационно-аналитической деятельности в сфере безопасности

http://profstandart.rosmintrud.ru

Соглашение о единых принципах и правилах обращения медицинских изделий (изделий медицинского назначения и медицинской техники) в рамках ЕврАзЭС, № 4-ФЗ от 31.01.2016

- единые правила в соответствии с рекомендациями Международного форума регуляторов медицинских изделий (IMDRF, www.imdrf.org, преемник GHTF)
- гармонизации (!) номенклатуры медицинских изделий (МИ) с Global Medical Device Nomenclature (GMDN, www.gmdnagency.org)
- информационная система ЕАЭС в сфере обращения МИ
  - единый реестр медицинских изделий
  - единый реестр уполномоченных организаций
  - единая база данных мониторинга безопасности, качества и эффективности медицинских изделий

Решения Коллегии ЕАЭС от 22.12.2015 г. № 173 (Классификация в зависимости от риска применения), № 174 (Мониторинг безопасности), от 29.12.2015 г. № 177 (Номенклатура)

Номенклатурная классификация медицинских изделий (МИ)

приказ Минздрава России от 06.06.2012 № 4н
в ред. приказа от 25.09.2014 № 557н (с 06.01.2015)

- **по видам** – www.roszdravnadzor.ru/services/mi_reesetr

Некоторые виды ПО отнесены к МИ !!

- **по классам** в зависимости от потенциального **риска применения** -> **классы: 1** (низкий), **2а, 2б, 3** (высокий риск)

Описаны правила определения класса риска для МИ:
а) контактирующих или воздействующих на пациента
б) используемых для диагностики in vitro (ИВД) (в т.ч. ПО)

"Самостоятельное" ПО, используемое совместно с МИ, имеет тот же класс риска, что и это МИ.

Для программных МИ (SaMD) правила определения класса риска в явном виде **не приведены** !!

При формальном применении правил для неинвазивных МИ (п.4.1) к программным МИ они всегда будут иметь низкий класс риска !? -> нужны официальные разъяснения !!

Отнесение ПО к медицинским изделиям (МИ) ->

- **обязательное подтверждение качества, эффективности и безопасности** – технические и клинические испытания (приказы Минздрава РФ от 09.01.2014 № 2н, от 15.08.2012 № 89н, от 21.12.2012 № 1353н в ред. приказа от 03.06.2015 г. № 303н)
- **государственная регистрация**, включение в госреестр медицинских изделий и организаций, осуществляющих их производство и изготовление (постановление Правительства РФ от 27.12.2012 г. № 1416, в ред. от 10.02.2017 № 160 – продление перерегистрации до 01.01.2021)
- **мониторинг безопасности** применения медицинских изделий (постановление Правительства РФ 25.09.2012 г. № 967, приказ Минздрава России от 14.09.2012 г. № 175н)

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

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

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

- управления работой медтехники (МТ) и мониторинга? за ее функционированием
- 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
- для 3D-моделирования
- связи диагностического и лечебного оборудования

Если ПО *не* предназначено для выполнения этих функций, то оно *не* является МИ ?!

ГОСТ ISO 14971-2011 Изделия медицинские. Применение менеджмента риска к медицинским изделиям

ГОСТ Р 55544-2013 Программное обеспечение медицинских изделий. Часть 1 Руководство по применению ИСО 14971 к программному обеспечению изделий

ГОСТ 30324.0.4-2002 Требования безопасности к программируемым медицинским электронным системам

ГОСТ Р МЭК 62304-2013 Изделия медицинские. Программное обеспечение. Процессы жизненного цикла

ГОСТ Р МЭК 62366-2013 Изделия медицинские. Проектирование медицинских изделий с учетом эксплуатационной пригодности

ГОСТ Р 55746-2013, 56032-2014 Изделия медицинские. Структура кодов для неблагоприятных событий

- **1101 – Проблема аппаратных средств компьютера (отказ *etc*)**
- **1102 – Проблема компьютерной сети, к которой подключено МИ**
- **1201 – Проблема прикладного ПО (неработоспособность, отказ) [12xx - ПО]**
- **1202 – Проблема программирования (некорректный результат расчета *etc*)**
- **2800 – Непредусмотренная функция (выдача некорректной информации *etc*)**
- **2805 – Безопасность ПО (отказ ПО МИ из-за недостаточной авторизации, контроля доступа и функций подотчетности)**

ГОСТ Р 56429-2015 (GHTF/SG5/N2R8:2007) Изделия медицинские. Клиническая оценка (*с 01.07.2016*)

ГОСТ Р 56606-2015 Контроль технического состояния и функционирования медицинских изделий. Основные положения (*с 01.09.2016*)

ГОСТ Р ИСО/ТС 25238-2009 Классификация угроз безопасности от медицинского программного обеспечения (ПО)

ГОСТ Р ИСО/ТО 27809-2009 Меры по обеспечению безопасности пациента при использовании медицинского ПО

IMDRF/SaMD WG/N10:2013 Software as a Medical Device: Key Definitions, 09.09.2013

IMDRF/SaMD WG/N12:2014 Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations, 18.09.2014

IMDRF/SaMD WG/N23:2015 Software as a Medical Device: Application of Quality Management System, 02.10.2015

IMDRF/SaMD WG (PD1)/N41R3 Software as a Medical Device: Clinical Evaluation, 05.08.2016 (принятие – сентябрь 2017)

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

Надо ли регистрировать "медицинское" ПО, указанное в письме от 30.12.2015, введенное в эксплуатацию до 06.01.2015 г.?

Как определить принадлежность к определенному номенклатурному виду МИ для многофункционального ПО?

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

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

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

Нужны разъяснения по поводу применения Решений ЕАЭС !!

Номенклатура медицинских изделий по видам

[приказ Минздрава России от 06.06.2012 г. № 4н]

232550 – Система телемедицинская для диагностической визуализации

234250 – Система для проведения видеоконференции для телемедицины

ГОСТ Р 57092-2016 Аппаратура для телемедицинских видеоконференций. Технические требования для государственных закупок (действует с 01.09.2017)

ГОСТ Р 57082-2016 Изделия медицинские электрические. Рабочая станция врача-рентгенолога. Технические требования для государственных закупок (действует с 01.09.2017)

Позиция Росстандарта по вопросу использования документов национальной системы стандартизации при применении положений федеральных законов от 18.07.2011 № 223-ФЗ и от 05.04. 2013 № 44-ФЗ – 25 января 2017 г.

[http://gost.ru/wps/portal/razyasnenie]

Проверки, контроль и надзор

О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля, № 294-ФЗ от 26.12.2008

Требования закона № 294-ФЗ с 01.09.2015 г. не распространяются на процедуры контроля и надзора за обработкой персданных !!

Порядок проверок Роскомнадзором устанавливается Правительством РФ (закон № 16-ФЗ от 22.02.2017)

Постановления Правительства РФ

О применении риск-ориентированного подхода при организации отдельных видов государственного контроля (надзора), от 17.08.2016 № 806 в ред. от 02.03.2017 № 245 -> + Росздравнадзор

Общие требования к разработке и утверждению проверочных листов (списков контрольных вопросов) -> публикация на сайте надзорного органа, от 13.02.2017 № 177 !!

Правила формирования и ведения единого реестра проверок, от 28.04.2015 г. № 415 -> сводный план и реестр проверок на сайте Генпрокуратуры РФ – www.genproc.gov.ru

"Проблемный лист" (предложения) (1)

На уровне федерального законодательства

- дистанционное оказание медицинской помощи – оказание телемедицинских (ТМ-) услуг "медицинский работник – пациент" (понятия: ТМ-услуга, ТМ-технологии, ТМ-система, "оператор ТМ-системы, условия и формы оказания ТМ-услуг *etc*)
- использования методов, технологий и процедур псевдонимизации (обезличивания) и обратной персонификации документированной информации, представленной в электронной форме, при ведении медицинских регистров, в том числе регистров потенциальных доноров органов и тканей, геномных (ДНК) и генетических регистров и иных медицинских (нозологических) регистров и полицевых баз данных, электронных хранилищ (цифровых архивов) медицинских документов (ИЭМК и др.) *etc*
- обеспечения достоверности и актуальности информации медицинского и фармацевтического характера, публикуемой на общедоступных интернет-сайтах

"Проблемный лист" (предложения) (2)

На уровне Правительства РФ

- требования и процедуры предоставления (оказания) услуг организациями системы здравоохранения в электронной форме (в том числе через личный кабинет "Мое здоровье" на ЕПГУ)
- порядок лицензирования деятельности и/или аккредитации организаций – медицинских организаций и операторов связи (провайдеров телематических услуг), осуществляющих и обеспечивающих оказание телемедицинских услуг
- требования к организациям – операторам ИС и порядок лицензирования деятельности, связанной с оказанием услуг по обработке, в том числе хранению и/или передаче, персонифицированной информации о состоянии здоровья с использованием интернет-сайтов и/или "облачных" технологий (например, по модели SaaS)
- создание отраслевого центра компетенции и мониторинга инцидентов в области кибербезопасности (MedCERT-RU)

"Проблемный лист" (предложения) (3)

На уровне Минздрава России (ст. 14, 91, 92 в № 323-ФЗ)

- порядок и условия ведения баз данных и иных информационных ресурсов в системе ОМС с учетом интеграции подсистем ЕГИСЗ с соответствующими ИС федерального и территориальных фондов ОМС и обмена данными со страховыми медицинскими организациями
- порядок ведения персонифицированного учета в электронной форме при осуществлении медицинской деятельности
- порядок ведения учетной медицинской документации в электронной форме (электронных медицинских документов), в том числе с использованием простой, усиленной неквалифицированной или квалифицированной электронной подписи медицинского работника
- порядок ведения и использования ИЭМК (как медицинского документа), в том числе с использованием процедур и технологий псевдонимизации и обратной персонификации
- включение ТМ-услуг в Номенклатру медицинских услуг

"Проблемный лист" (предложения) (4)

На уровне Минздрава России (ст. 14, 91, 92 в № 323-ФЗ)

- порядки оказания ТМ-услуг, включая правила идентификации и аутентификации медицинских работников и пациента, а также правила документирования ТМ-услуг
- оформления информированного добровольного согласия пациента на медицинское вмешательство с учетом потенциальных рисков применения ТМ-технологий
- порядки ведения нозологических и иных медицинских регистров на основе применения унифицированных технологий и процедур, и получения данных из ИЭМК
- критерии отнесения ПО, предназначенного для автоматизации лечебно-диагностического процесса, к медицинским изделиям (программным медицинским изделиям, SaMD)
- правила определения потенциального риска применения для программных медицинских изделий

"Проблемный лист" (предложения) (5)

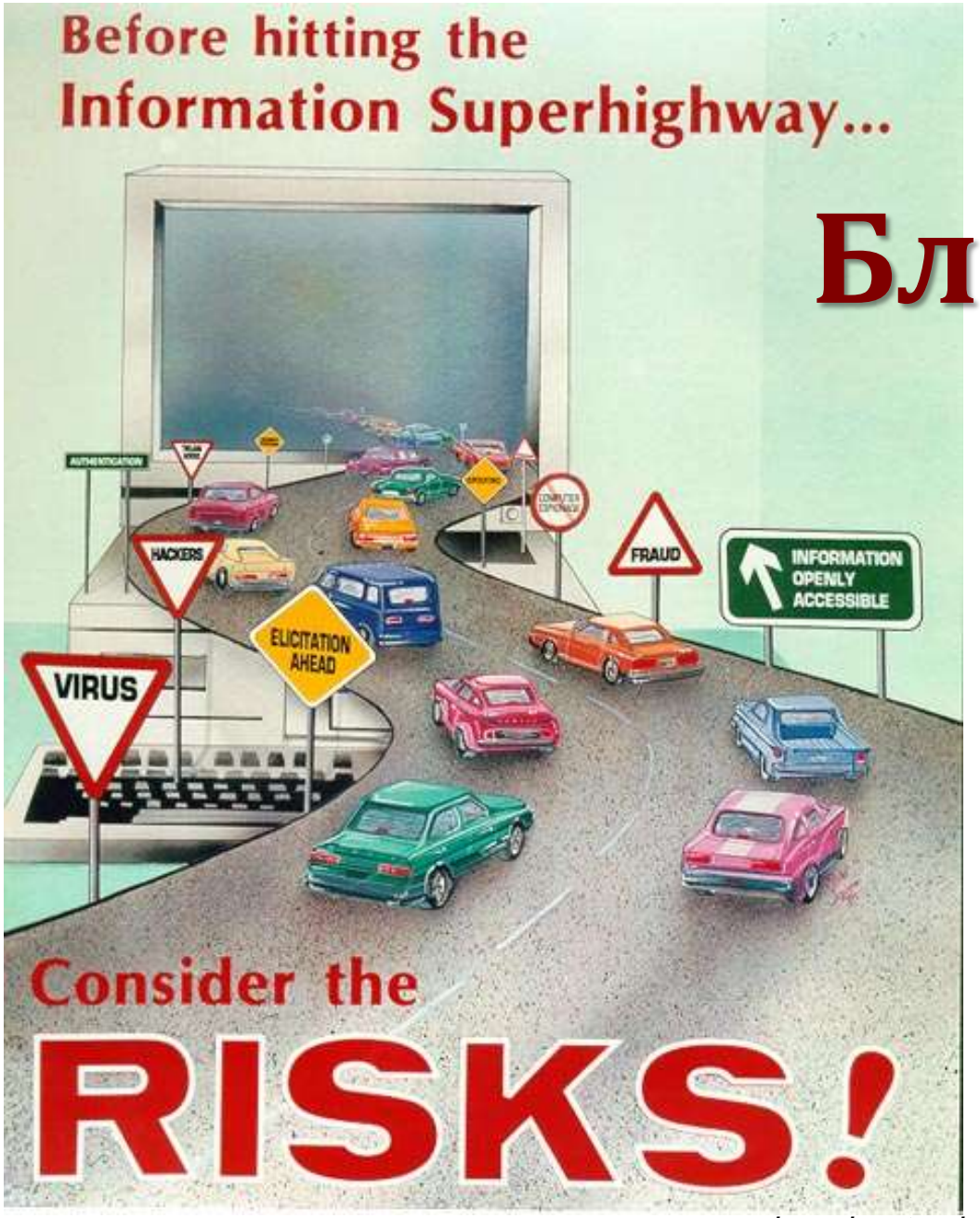
На уровне Минздрава России (ст. 14, 91, 92 в № 323-ФЗ)

- правила определения классов киберзащищенности цифровой медицинской техники
- требования к средствам и правила идентификации и аутентификации цифровой медицинской техники в едином информационном пространстве системы здравоохранения
- типовая интегральная модель угроз информационной безопасности + рекомендации по защите (персональных данных, МИС, электронных документов, медицинской техники)
- порядок разработки и ведения единой системы классификаторов и справочников и иной НСИ, используемой для идентификации, кодирования и обработки информации, в том числе выполнения медико-экономических расчетов в системе здравоохранения и ОМС
- уточнение нормативов, используемых при планировании сети медицинских организаций, табелей оснащения, определения штатной численности персонала, с учетом применения ИКТ

За безопасность надо платить, в противном случае придётся расплачиваться ...

Уинстон Черчиль

Luis Ayala. Cybersecurity for Hospitals and Healthcare Facilites. A Guide to Detection and Prevention.
ISBN 978-1-4842-2155-6, Apress, 2016, 129 p.



www.wrc.noaa.gov/wrso/posters/

Благодарю за внимание! Вопросы?

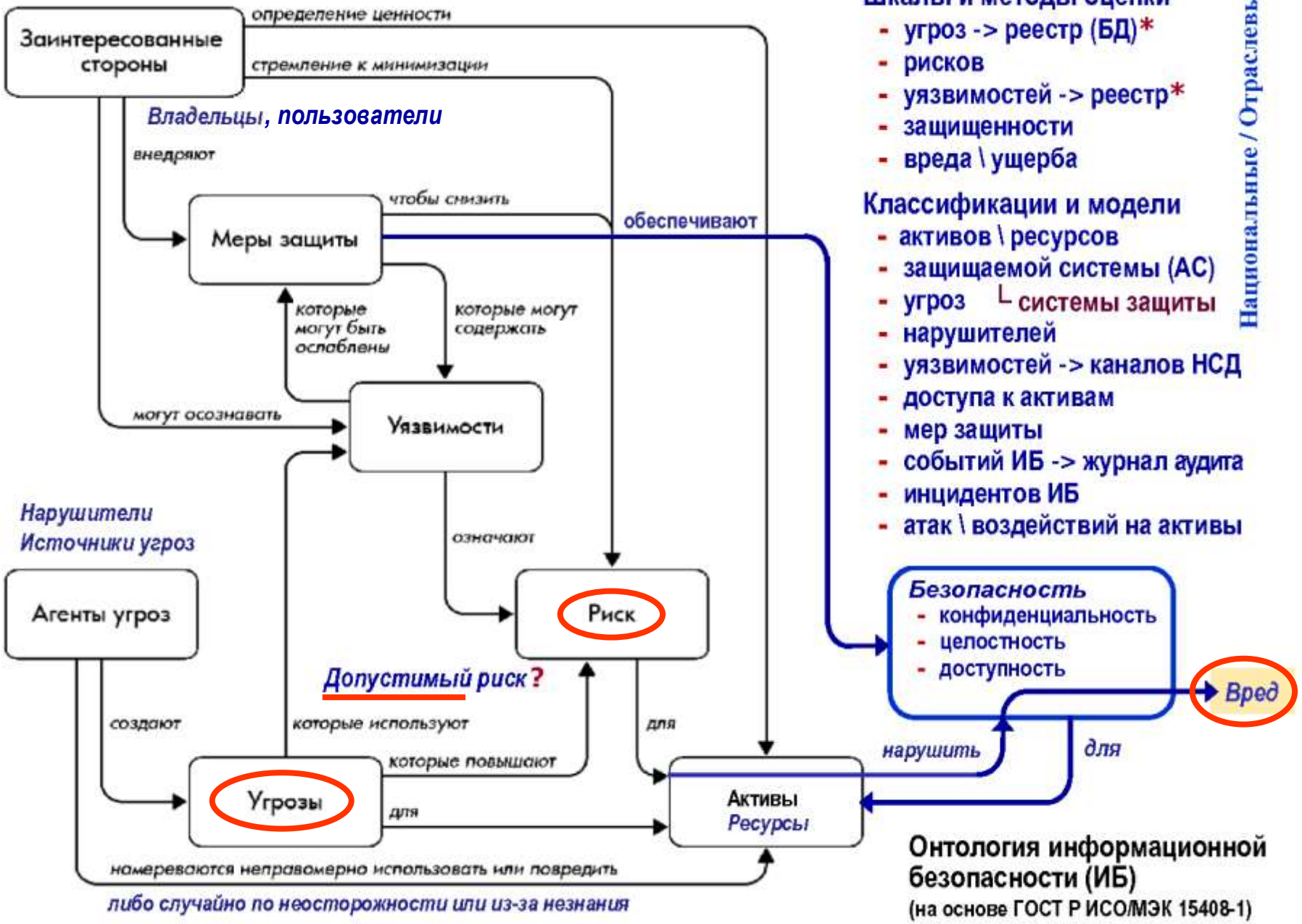
Столбов Андрей Павлович

ap100Lbov@mail.ru

Информационные технологии как фактор доступности, безопасности, качества и эффективности медицинской помощи

Россия использует примерно 30% современных медицинских технологий, доступных в мировом здравоохранении

"Известия", 30 марта 2017


Заинтересованные стороны
определение ценности
стремление к минимизации
Владельцы, пользователи
внедряют
Меры защиты
чтобы снизить
обеспечивают
которые могут быть ослаблены
которые могут содержать
могут осознавать
Уязвимости
означают
Нарушители
Источники угроз
Агенты угроз
Риск
Допустимый риск?
создают
которые используют
для
которые повышают
Угрозы
для
Активы
Ресурсы
намереваются неправомерно использовать или повредить
либо случайно по неосторожности или из-за незнания
нарушить
для
Безопасность
- конфиденциальность
- целостность
- доступность
Вред
Шкалы и методы оценки
- угроз -> реестр (БД)*
- рисков
- уязвимостей -> реестр*
- защищенности
- вреда \ ущерба
Классификации и модели
- активов \ ресурсов
- защищаемой системы (АС)
- угроз └ системы защиты
- нарушителей
- уязвимостей -> каналов НСД
- доступа к активам
- мер защиты
- событий ИБ -> журнал аудита
- инцидентов ИБ
- атак \ воздействий на активы
Национальные / Отраслевые
Онтология информационной безопасности (ИБ)
(на основе ГОСТ Р ИСО/МЭК 15408-1)

Концепция создания единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ), ***приказ Минздравсоцразвития России от 28.04.2011 № 364***

http://portal.egisz.rosminzdrav.ru – портал ЕГИСЗ

Общие принципы построения и функционирования информационных систем и порядок информационного взаимодействия в сфере ОМС (АИС ОМС), ***приказ ФОМС № 79 от 07.04.2011 г. (в ред. приказа № 276 от 26.12.2013 г.)***

Методические рекомендации по обеспечению функциональных возможностей МИС медицинских организаций (МИС МО), ***Утверждены Министром здравоохранения РФ 01.02.2016 г.***

Методические рекомендации по обеспечению функциональных возможностей региональных МИС (РМИС), ***Утверждены Министром здравоохранения РФ 23.06.2016 г.***

Основные разделы электронной медицинской карты (ЭМК), ***утвержден Министром здравоохранения РФ 11.11.2013 г.***

Государственная программа развития здравоохранения РФ

постановление Правительства РФ от 15.04.2014 г. № 294

Подпрограмма Г **"Управление развитием отрасли" –** Г.2 Информатизация здравоохранения, включая развитие телемедицины

Приоритетный проект (Совет по стратегическому развитию, 25.10.2016)

Совершенствование процессов организации медицинской помощи на основе внедрения информационных технологий, до 2025г. ("Электронное здравоохранение") -> контрольные показатели:

- имеют личный кабинет "Мое здоровье": 2017 – 6 млн., 2018 – 14 млн., 2015 – 48 млн. граждан
- доля застрахованных по ОМС граждан, для которых заведены ЭМК: 2016 – 30%, 2017 – 40%, 2018 – 100%
- доля амбулаторно-поликлинических МО, внедривших МИС и перешедших на ведение электронной медицинской документации: 2017 – 30%, 2018 – 40%, 2025 – 99%
- число субъектов РФ, в которых организовано оказание медицинской помощи с применением телемедицинских технологий, в соответствии с требованиями Минздрава России: 2017 – 7, 2018 – 20, 2025 – 85 *etc*

Национальная технологическая инициатива ХелсНет (28.12.2016, www.sntr-rf.ru)

Концепция создания федеральной государственной информационной системы мониторинга движения лекарственных препаратов от производителя до конечного потребителя с использованием маркировки (ФГИС МДЛП), приказ Минздрава РФ от 30.11.2015 № 866

О проведении эксперимента по маркировке контрольными (идентификационными) знаками и мониторингу за оборотом отдельных видов лекарственных препаратов для медицинского применения, постановление Правительства РФ от 24.01.2017 № 62

Методические рекомендации для проведения эксперимента (Минздрав РФ, 28.02.2017) (оператор ФГИС МДЛП – ФНС России)

Приоритетный проект (Совет по стратегическому развитию, 25.10.2016)

Внедрение автоматизированной системы мониторинга движения лекарственных препаратов производителя до конечного потребителя для защиты населения от фальсифицированных препаратов и оперативного выведения из оборота контрафактных и недоброкачественных препаратов, до 01.03.2019

ГОСТ Р ИСО 11238, 11239, 11240, 11615, 11616, ГОСТ Р 57305 – идентификация и описание лекарственных средств (ISO)

UNISCAN / GS1 Russia – идентификация товаров – www.gs1ru.org

Телемедицинские технологии – комплекс организационных, технических и иных мер, применяемых в процессе оказания медицинской помощи пациенту с использованием процедур, средств и способов передачи данных по линиям связи, обеспечивающих достоверную идентификацию участников информационного обмена, медицинского работника и пациента

Телемедицинская услуга – ***медицинская услуга***, выполняемая ***дистанционно*** с использованием телемедицинских технологий

Медико-информационные услуги (сервисы) – использование электронной почты,"личного кабинета" на сайте, SMS или иных способов передачи сообщений по каналам связи для:

- записи на прием к врачу, на плановую госпитализацию и т.д.
- уведомления пациента о дате и времени приема, дате госпитализации, готовности результатов обследования, напоминание о приёме лекарственного препарата, измерении давления и т.д. (на основании соглашения с пациентом !!)
- запроса и получения электронных копий медицинских документов, рецептов и т.д.

Каковы особенности обеспечения кибербезопасности (КБ) в здравоохранении – защиты медицинской техники, МИС, персональных данных *etc*?

Кто должен заниматься разработкой проектов нормативно-методических документов в области

- кибербезопасности МИС, медицинской техники (определять требования к защищенности, классификации, состав мер по нейтрализации угроз и т.д.)?
- безопасности применения медицинского ПО в клинической практике?

Кто должен осуществлять контроль (надзор) и мониторинг

- кибербезопасности МИС и МТ в медицинских организациях?
- безопасности применения медицинского ПО?

Дефицит специалистов в области КБ -> нужен отраслевой центр компетенции и мониторинга инцидентов КБ !!

- **Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки только при наличии согласия субъекта в письменной форме или в случаях, предусмотренных федеральными законами ...**
- **Оператор обязан разъяснить субъекту порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражения против такого решения ...**
- **Оператор обязан рассмотреть возражение в течение 30 дней и уведомить субъекта о результатах такого возражения**

[ст. 16 закона № 152-ФЗ]

Что понимать под *"исключительно автоматизированной обработкой ..."* ?? Может быть все-таки "*автоматической*", без участия человека (ЛПР) ?!

Приказы ФСТЭК – требования, 6 классов защиты СрЗИ:

- к средствам обнаружения вторжений – № 638 от 06.12.2011
- к средствам антивирусной защиты – № 28 от 20.03.2012
- к средствам доверенной загрузки – № 119 от 27.09.2013
- к средствам контроля съемных машинных носителей информации – № 87 от 28.07.2014
- к межсетевым экранам – № 9 от 09.02.2016, профили – 12.09.2016
- к операционным системам – № 119 от 19.08.2016

Проект приказа ФСТЭК о внесении изменений в приказы № 21, № 31

- требования к классам защиты, используемых СрЗИ
- возможность сертификации СрЗИ на соответствие ТУ, заданиям по ИБ (было – только РД)

Требования к обеспечению защиты информации в АСУ производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (приказ ФСТЭК от 14.03.2014 № 31)

Информационное сообщение ФСТЭК от 25.07.2014 № 240/22/2748 по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14.03.2014 № 31

Требования к защите персональных данных при их обработке в информационных системах персональных данных (постановление Правительства РФ от 01.11.2012 № 1119)

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (приказ ФСТЭК от 18.02. 2013 № 21)

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) (ФСТЭК, 2008)

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (ФСТЭК, 2008)

Информационное сообщение ФСТЭК от 20.11.2012 № 240/24/4669 о сертификации средств защиты информации для ИСПДн

Информационное сообщение ФСТЭК от 15.07.2013 № 240/22/2637 в связи с изданием приказов № 17 и № 21 ?!

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИС персональных данных с использованием средств **криптографической защиты** информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности **(приказ ФСБ от 10.07.2014 № 378)**

Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИС персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности **(утверждены ФСБ 31.03.2015, № 149/7/2/6-432)**

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 **!?**

Решения Коллегии ЕАЭС от 22.12.2015 г. № 173 – Классификация в зависимости от риска применения

Самостоятельное программное обеспечение (SaMD ?!) рассматривается как **активное медицинское изделие** -> экстраполяция правил определения класса риска (КР) для аппаратов и приборов на самостоятельное ПО

Назначение ПО:

диагностическое ("прибор"), терапевтическое ("аппарат")

Применение ПО для:

а) контроля / управления? активным терапевтическим МИ:
- неимплантруемым => КР = 2а (2б) в зависимости от $КР_{МИ}$
- имплантируемым => КР = 3

б) контроля параметров
- жизненно важных функций => КР = 2а
- сердца, ЦНС, ЦСК, дыхания => КР = 2б

Во всех остальных случаях => КР = 1 (низкий риск)

Правила государственной регистрации медицинских изделий, *постановление Правительства РФ № 1416 от 27.12.2012*

Положение о государственном контроле за обращением медицинских изделий, *постановление Правительства РФ № 967 от 25.09.2012*

Положение о лицензировании деятельности по производству и техническому обслуживанию (за исключением случая, если тех.обслуживание осуществляется для обеспечения собственных нужд ...) медицинской техники, *постановление Правительства РФ № 469 от 03.06.2013*

Порядок осуществления мониторинга безопасности медицинских изделий, *приказ Минздрава России № 175н от 14.09.2012*

Порядок проведения испытаний в целях утверждения типа средств измерений, а также перечня медицинских изделий, относящихся к средствам измерений ... в отношении которых проводятся испытания в целях утверждения типа средств измерений, *приказ Минздрава России № 89н от 15.08.2012*

ГОСТ Р ИСО 15225-2014 (ISO:2010) Структура данных номенклатуры медицинских изделий

ГОСТ 31508-2012 Изделия медицинские. Классификация в зависимости от потенциального риска применения. Общие требования

ГОСТ Р 51088-2013 Медицинские изделия для диагностики ин витро. Реагенты, наборы реагентов, тест-системы, контрольные материалы, питательные среды. Требования к изделиям и поддерживающей документации

ГОСТ Р ИСО/ТО 22790-2009 Функциональные характеристики систем поддержки назначений лекарств

ГОСТ Р 8.654-2015 Требования к программному обеспечению средств измерений

ГОСТ Р ИСО/МЭК 18045-2013 Методология оценки безопасности информационных технологий

ГОСТ Р ИСО/МЭК 15408-3-2013 Критерии оценки безопасности информационных технологий. Часть 3 Компоненты доверия к безопасности

Об основах охраны здоровья граждан в Российской Федерации, *№ 323-ФЗ от 21.11.2011*

О персональных данных, *№ 152-ФЗ от 27.07.2006*

Об информации, информационных технологиях и о защите информации, *№ 149-ФЗ от 27.07.2006*

Об электронной подписи, *№ 63-ФЗ от 06.04.2011*

О техническом регулировании, *№ 184-ФЗ от 27.12.2002*

О стандартизации в Российской Федерации, *№ 162-ФЗ от 29.06.2015* **(действует с 01.07.2016) !!!**

Об обеспечении единства измерений, *№ 102-ФЗ от 26.06.2008*

Об аккредитации в национальной системе аккредитации, *№ 412-ФЗ от 28.12.2013*

Global Harmonization Task Force (GHTF) – www.imdrf.org

Медицинскими изделиями являются любые инструменты, аппараты, приборы, оборудование, материалы и прочие изделия, применяемые в медицинских целях отдельно или в сочетании между собой, а также *вместе с другими* ***принадлежностями****, необходимыми для применения указанных изделий по назначению, включая* ***специальное*** *программное обеспечение,* и **предназначенные производителем** для профилактики, диагностики, лечения и медицинской реабилитации заболеваний, мониторинга состояния организма человека, проведения медицинских исследований, восстановления, замещения, изменения анатомической структуры или физиологических функций организма ... функциональное назначение которых не реализуется путем фармакологического, иммунологического, генетического или метаболического воздействия на организм ...

Медицинские изделия подразделяются на **классы** в зависимости от **потенциального риска их применения** и на **виды** в соответствии с номенклатурной классификацией мед.изделий ...

[ст. 38 закона № 323-ФЗ "Об основах охраны здоровья ..."]

157300 – Прикладное ПО ИС для ведения карты пациента – прикладная программа, подпрограммы и/или алгоритмы для применения в качестве или в составе ИС для электронного получения, сбора, хранения, управления, помощи в анализе, отображения, выведения и распространения [?] данных в пределах или между медицинскими учреждениями, чтобы поддерживать электронную регистрацию и ведение электронных историй болезни пациентов. ПО позволяет мед.работникам пересматривать и обновлять записи в мед.картах пациентов, размещать предписания (например, для лекарственных средств, процедур, тестов) и иногда комплексные данные, полученные от различных специалистов <...>

157610 – Прикладное ПО информационной административной системы учета пациентов – прикладная программа <...> чтобы поддерживать службы учета пациентов. Данные обычно содержат демографическую информацию о пациенте, о его приеме, выписке, переводе и амбулаторном лечении <...>

182990 – Прикладное ПО для кодирования клинической информации – прикладная компьютерная программа <...> для поддержания административной и клинической деятельности, связанной с электронной регистрацией диагнозов пациента и полученных им процедур. Данные используются для внесения поправок в демографические и клинические данные, определения группы сходного диагноза и уровня клинической сложности пациента <...>

325070 – Прикладное программное обеспечение для поддержки клинического ведения пациента на основе веб-приложений – Прикладная программа предназначена для обеспечения принятия решений, касающихся клинического ведения пациента, на основе получения структурированных данных о пациенте из электронной истории болезни (например, демографические данные, диагностика, результаты лабораторных исследований) и возвращения информации о клиническом уходе (например, напоминания, рекомендации и ссылки на руководящие указания) медицинскому работнику, осуществляющему контроль за пациентом. Она также известна как ПО для **поддержки принятия клинических решений**. Она функционирует как веб-служба (программа, работающая на веб-сервере, взаимодействующая с другим программным обеспечением, но не имеющая собственного пользовательского интерфейса) -> *SaaS (в ЕГИСЗ)*

232550 – Система телемедицинская для диагностической визуализации – комплект изделий для электронной передачи цифровых радиологических изображений, например, магнитно-резонансное изображение, рентген, ультразвук, эндоскопия или компьютерная томография, а также телерентгенография. Обычно информация передается по общедоступным каналам, телефонным линиям или микроволнам. Система изначально отличается от системы **архивации** и **передачи** изображения (САПИ) объёмом памяти компьютера и использованием по назначению. САПИ – это объёмная система запоминающих устройств, контролируемого хранения файлов и извлечения тысяч образов, тогда как телерентгенографическая система имеет объём памяти, рассчитанный на менее чем 1000 изображений

САПИ = PACS – Picture Archiving and Communication System

Прикладное ПО системы хранения и передачи изображений в дерматологии (130760), для виртуальной бронхоскопии (293280)

234250 – Система для проведения видеоконференции для телемедицины – универсальная система, используемая внутри телемедицинской зоны для дистанционного оказания практической медицинской помощи в режиме реального времени с использованием компьютерных сетей и средств видеоконференцсвязи внутри больницы, между больницами, а также ***для национальных и международных конференций.***

Видеоконференция с участием субъекта (медработника, парамедика, пациента), находящегося вне медицинской организации (больницы) **!?**

Включает видеокамеру, аудиооборудование (микрофон, динамик), программное обеспечение, телекоммуникацинное оборудование, компьютер **!?**

181280 – Прикладное ПО для информационной системы клинической лаборатории – прикладная программа, подпрограммы и/или алгоритмы для применения в качестве или в составе информационной системы для электронного получения, сбора, хранения, управления, ***помощи в анализе***, отображения, выведения и распространения данных в пределах или между медицинскими учреждениями, чтобы поддерживать административную и медицинскую деятельность, связанную с обеспечением работы клинической лаборатории <...>

ГОСТ Р 53798-2010 Стандартное руководство по лабораторным информационным менеджмент-системам (ASTM E 1578 LIMS)

ГОСТ Р 54360-2011 Лабораторные информационные менеджмент-системы (ЛИМС). Стандартное руководство по валидации ЛИМС (ASTM E 2066 LIMS)

Исключить из Номенклатуры

157300 – Прикладное ПО информационной системы для ведения карты пациента

157610 – Прикладное ПО информационной административной системы учета пациентов

181990 – Прикладное ПО для кодирования клинической информации

183250 – Прикладное ПО информационной системы для управления профессиональной деятельностью врачей

216160 – Прикладное ПО информационной системы управления рисками

311960 – Прикладное ПО для конфигурируемой электронной медицинской карты пациента на основе веб-приложений

137130 – Прикладное ПО информационной системы учета медицинских изделий

234250 – Система для проведения видеоконференции для телемедицины [HW + SW ?]

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**

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (приказ ФСТЭК от 18.02. 2013 № 21)

Требования к обеспечению защиты информации в АСУ производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (приказ ФСТЭК от 14.03.2014 № 31)

Приказы ФСТЭК – требования, 6 классов защиты:

- к операционным системам – № 119 от 19.08.2016
- к межсетевым экранам – № 9 от 09.02.2016, профили – 12.09.2016

Проект приказа ФСТЭК о внесении изменений в приказы № 21, № 31

- требования к классам защиты СрЗИ
- возможность сертификации СрЗИ по ТУ, заданиям по ИБ (было - по РД)

Информационное сообщение ФСТЭК от 15.07.2013 № 240/22/2637 в связи с изданием приказов № 17 и № 21 ?!

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