ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕДИЦИНЕ
ИТМ 2019

Кибербезопасность как фактор доступности, безопасности, качества и эффективности медицинской помощи.
Кибербезопасность как осознанная необходимость

Обеспечение кибербезопасности в здравоохранении: обзор последних нормативных актов

Сеченовский Университет
ВЫСШАЯ ШКОЛА УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ
www.hsha.ru

Столбов Андрей Павлович

Москва, 10 октября 2019 г.

Проблемы надежной аутентификации субъектов -> eID, BiometricsID, Digital Signature, Digital Certificate, доверенная третья сторона *etc*

Главврач Тюменского федерального центра нейрохирургии Альберт Суфианов сообщил о хакерской атаке на его учреждение, которая случилась во время операции на головном мозге 13-летней девочки. Все приборы, которые сопровождали операцию, были отключены. Врачи сумели довести операцию до конца фактически без показаний приборов и снимков на мониторах. По его просьбе Г. Греф направил в клинику специалистов Сбербанка, которые провели идентификацию вируса и восстановили работоспособность систем.

Как отмечают аналитики, медицинские данные на "черном рынке" оцениваются в 10–15 раз дороже паспортных данных. [ТАСС, 6 июля 2018]

По данным Министерства здравоохранения и социальной защиты Великобритании причиненный Национальной системе здравоохранения (NHS) ущерб от кибератаки с использованием вируса WannaCry в 2017 г. составил £92 млн. Из-за кибератаки была нарушена работа трети госпиталей NHS и 8% клиник врачей общей практики, отменено более 19 тыс. записей на прием к врачу.

[Коммерсантъ, 12 октября 2018]

Серию кибератак на десяток крупных госучреждений здравоохранения в южных регионах страны зафиксировала весной и летом текущего года "Лаборатория Касперского". Русскоговорящих хакеров интересовали финансовые документы. Удаленное проникновение в компьютеры производилось с помощью программы-шпиона CloudMid, которая рассылалась по электронной почте. Своей цели хакеры достигли и нужные данные получили.

[Медвестник, 18 июля 2019]

Взлом ЕПГУ (февраль 2015, июль 2017, январь 2019 - Kaspersky Lab, habr.com)

Блокировка SSL-сертификата **сайта ОНФ** (GeoTrust, 4 июня 2018)

Утечка конфиденциальной информации за 2018 (InfoWatch, 30.05.2019)

- **23.3%** госорганы
- **12.2%** банки и платежные системы
- **10.4%** телеком
- **8.5%** медицинские организации (21.7% "заказ")
- **5.6%** торговля
- **42.7%** через браузер и облачные сервисы
- **44.6%** через "бумагу"
- **1.5%** через смартфон
- **3.3%** через электронную почту
- **0.9%** через "флешки"

78% инцидентов из-за **низкой организации**, **незнания** и **халатности**

52% не видят угроз в утечке их персональных данных (ВЦИОМ, 11.2018)

Сокрытие информации об инцидентах нарушения ИБ **!!**

Конвенция Совета Европы от 28.01.1981 "О защите физических лиц при автоматизированной обработке персональных данных", протокол EST № 108, ратифицирована законом № 160-ФЗ от 19.12.2005

10.10.2018 РФ подписала протокол изменений в EST № 108 от 18.05.2018

О персональных данных, № 152-ФЗ от 27.07.2006 (ред. от 31.12.2017)

Об информации, информационных технологиях и о защите информации, № 149-ФЗ от 27.07.2006 (ред. от 01.05.2019)

О безопасности критической информационной инфраструктуры (КИИ) Российской Федерации, № 187-ФЗ от 26.07.2017

Законопроекты об обработке персональных данных (2018-2019)

- о ратификации Протокола № 108 – 17.09.2019
- персональные генетические данные (нов. ред. Протокола № 108)
- уведомление оператором субъекта персональных данных и уполномоченных органов об утечке данных (нов. ред. Протокола № 108)
- требования к уничтожению персональных данных и обработке обезличенных данных – 01.08.2019, 18.09.2019
- особенности обработки и защиты персональных данных, полученных из биологического и генетического материала человека
- цифровой профиль гражданина и юридического лица в ЕСИА

Постановления Правительства РФ (1)

Правила организации и осуществления государственного контроля и надзора за обработкой персональных данных, № 146 от 13.02.2019

Правила категорирования и критерии значимости объектов КИИ, № 127 от 08.02.2018 (ред. от 13.04.2019 № 452)

– госорганам и госучреждениям до 01.09.2019 утвердить перечень объектов КИИ

Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ "О персональных данных" ... операторами, являющимися государственными или муниципальными органами, №_211 от 21.03.2012 (ред. от 15.04.2019 № 454)

Правила идентификации пользователей сети Интернет организатором сервиса обмена мгновенными сообщениями, № 1279 от 27.10.2018 (с 05.05.2019)

Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных ИС и дальнейшего хранения содержащейся в их базах данных информации, № 676 от 06.07.2015 (ред. от 07.08.2019 № 1026)

Постановления Правительства РФ (2)

Состав сведений, размещаемых в единой ИС персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина РФ, включая вид биометрических персональных данных, № 772 от 30.06.2018 (ред. от 13.09.2019 № 1197)

См. приказ Минкомсвязи РФ от 25.06.2018 № 321 (в ред. пр. № 369 от 04.07.2019)

Форма согласия на обработку персональных данных, необходимых для регистрации гражданина в ЕСИА, и иных сведений, если такие сведения предусмотрены фед. законами в указанной системе, и биометрических персональных данных в единой ИС персональных данных (ЕБС), № 1322-р от 30.06.2018 (ред. от 13.09.2019 № 2063-р)

Требования к антитеррористической защищенности объектов, относящихся к сфере деятельности Минздрава РФ, № 8 от 13.01.2017 (ред. от 29.03.2019 № 357)

е) организация обеспечения информационной безопасности *etc*

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, приказ ФСТЭК от 11.02.2013 № 17 (в ред. приказа № 106 от 28.05.2019)

Постановления Правительства РФ (3)

Правила взаимодействия иных ИС, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности мед. организаций и предоставляемых ими услуг, с ИС в сфере здравоохранения и медицинскими организациями,
№ 447 от 12.04.2018 (ред. от 02.02.2019 № 77)

Положение о единой государственной информационной системе в сфере здравоохранения (ЕГИСЗ), № 555 от 05.05.2018 (ред. от 02.02.2019 № 77)

Требования к государственным ИС в сфере здравоохранения субъектов РФ, медицинским ИС медицинских организаций, ИС фармацевтических организаций, приказ МЗ РФ № 911н от 24.12.2018

Порядок организации и оказания медицинской помощи с применением телемедицинских технологий, приказ МЗ РФ № 965н от 30.11.2017

Порядок обезличивания сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, осмотры и освидетельствования, приказ МЗ РФ № 341н от 14.06.2018

Общие принципы построения и функционирования информационных систем и порядок информационного взаимодействия в сфере ОМС, приказ ФОМС № 79 от 07.04.2011 (ред. от 13.12.2018 № 285) – псевдонимизация запроса к ЕРЗ

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

- Организационно-распорядительные документы по безопасности значимых объектов разрабатываются исходя из особенностей деятельности субъекта КИИ (п. 24)

  – Методические документы от Минздрава РФ !?
- Документы должны регламентировать, в том числе правила безопасной работы и действия персонала при возникновении компьютерных инцидентов и иных нештатных ситуаций (п. 25) -> киберучения !!
- Применяемые средства защиты информации должны быть обеспечены гарантийной, технической поддержкой со стороны производителей (п. 21)

Требования по обеспечению безопасности значимых объектов КИИ, приказ ФСТЭК от 25.12.2017 № 239 (в ред. пр. от 21.03.2019 № 60)

- Модель угроз безопасности объектов КИИ
- Должно быть подтверждено, что в объекте КИИ, отсутствуют уязвимости, содержащиеся в Банке данных угроз ФСТЭК или выявленные уязвимости не приводят к возникновению угроз объекту КИИ (п. 12.6)
- Состав мер по обеспечению безопасности объектов КИИ (для 3-х категорий)

www.bdu.fstec.ru, угроз – 213, уязвимостей – 23017, на 03.10.2019

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

Форма направления сведений о результатах присвоения объекту КИИ категории значимости, приказ ФСТЭК от 22.12.2017 № 236 (в ред. пр. от 21.03.2019 № 59)

Национальный координационный центр по компьютерным инцидентам, приказ ФСБ от 24.07.2018 № 366 www.cert.gov.ru

Перечень и порядок предоставления информации в ГосСОПКА, приказ ФСБ от 24.07.2018 № 367

Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ. Порядок получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения, приказ ФСБ от 24.07.2018 № 368

Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, приказ ФСБ от 06.05.2019 № 196

Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, приказ ФСБ от 19.06.2019 № 281

Порядок информирования ФСБ о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ, приказ ФСБ от 19.06.2019 № 282

Об организации работы по внедрению и применению информационных технологий. Приказ Минздрава РФ от 08.10.2018 № 687

В целях совершенствования эффективности реализации госпрограммы "Развитие здравоохранения", соблюдения требований закона № 187-ФЗ "О безопасности критической информационной инфраструктуры ...", а также реализации мероприятий по координации информатизации федеральных учреждений, находящихся в ведении Минздрава России

- создать на базе ФГБУ ВЦМК "Защита" Федеральный ресурсный центр по внедрению и применению информационных технологий (Центр)
- установить основными задачами Центра
  - создание и развитие ИС и компонентов ИТК-инфраструктуры в пределах установленной компетенции Центра и по поручению Минздрава РФ
  - проведение работ по обеспечению информационной безопасности Минздрава РФ, включая обеспечение безопасности объектов КИИ
  - проведение экспертизы в сфере ИТК-технологий по поручению Минздрава РФ, включая экспертизы документов, поставленных товаров, результатов выполненных работ и услуг, программ для ЭВМ и баз данных, и техдокументации
  - проведение экспертной оценки документов, используемых при планировании, создании и использовании ИТК-технологий в деятельности учреждений, находящихся в ведении Минздрава РФ

Министерства по согласованию с ФСТЭК могут устанавливать дополнительные требования к защите объектов КИИ с учетом особенностей их сферы деятельности (ст. 11 закона № 187-ФЗ)

Министерства, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности перс.данных, актуальные при их обработке в ИС, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания перс.данных, характера и способов их обработки (ч. 5 ст. 19 закона № 152-ФЗ)

Отраслевая интегральная модель угроз (комплекс моделей)

Новый комплект нормативно-методических документов (как в декабре 2009)

www.kmiac.ru – МИАЦ Красноярского края

www. www.brkmed.ru/category/miac/ – МИАЦ Брянской обл.

www.miac.nnov.ru – МИАЦ Нижегороской обл.

Методические рекомендации по категорированию объектов КИИ, принадлежащих субъектам КИИ, функционирующим в сфере связи (решение Исполкома "Ассоциации документальной электросвязи" от 26.06.2019. Согласованы с 8 Центром ФСБ (исх.№ 149/2/7- 370 от 05.04.2019), с ФСТЭК (исх.№ 240/25/1221 от 18.03.2019)

U.S. Department of Health & Human Services, December 28, 2018

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)
- Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations
- Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations
- Resources and Templates: The Resources and Templates portion includes a variety of cybersecurity resources and templates for end users to reference

[https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx]

Postmarket Management of Cybersecurity in Medical Devices. Guidance for Industry and FDA Staff, December 2016 (ed. 10/01/2018)

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Guidance for Industry and FDA Staff, October 2014, DRAFT (ed. 10/18/2018)

Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. Guidance for Industry, January 2005 (ed. 02/02/2018)

www.fda.gov

IMDRF/CYBER WG/N 60 Principles and Practices for Medical Device Cybersecurity. DRAFT. – October 1, 2019 – December 2, 2019 www.imdrf.org

ГОСТ Р 58412-2019 Защита информации. Разработка безопасного программного обеспечения (ПО). Угрозы безопасности при разработке ПО

ГОСТ 34.10, 34.11-2018 Криптографическая защита информации. – Процессы формирования и проверки электронной подписи. – Функция хэширования.

ГОСТ Р ИСО/МЭК 29161-2019 Информационные технологии. Структура данных. Уникальная идентификация для интернета вещей

ГОСТ Р МЭК 82304-1-2019 Медицинское программное обеспечение. Часть 1. Общие требования к безопасности программных продуктов / IEC:2016

ГОСТ Р ИСО/HL7 16527-2019 Функциональная модель HL7 системы ведения персональных электронных медицинских карт. Выпуск 1 (ФМ СВ ПЭМК)

ГОСТ Р ИСО/HL7 10781-2019 Функциональная модель HL7 системы ведения электронных медицинских карт. Выпуск 2 (ФМ СВ ЭМК)

ГОСТ Р ИСО 17523-2019 Требования к электронным рецептам

ГОСТ Р 58502-2019 Автоматическая идентификация, маркировка и этикетировка при сборе данных. Идентификация субъектов и индивидуальных поставщиков медицинской помощи

Перечень стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки ЕАЭС, Рекомендации Коллегии ЕАЭК от 12.03.2019 № 9

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 /* ISO/TS 11633-1:2019

Применение технологии **LPS** (Lightweight Portable Security) на основе LiveUSB для создания VPN-клиентов, защищенных АРМ, работы с электронными документами – **http://spi.dod.mil**

Благодарю за внимание !
Вопросы ?

Столбов Андрей Павлович

ap100Lbov@mail.ru

www.hsha.ru

Сеченовский Университет

ВЫСШАЯ ШКОЛА УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ

Федеральный проект "Нормативное регулирование цифровой среды"

Утвержден Советом по стратегическому развитию 24.12.2018, протокол № 16

До 31 июля 2019 должны быть приняты федеральные законы:

1.1. Регулирующие механизмы формирования и использования "облачной" электронной подписи (ЭП), установление унифицированных требований к универсальной (единой) усиленной квалифицированной ЭП (УКЭП), визуализацию ЭП, уточнение правового статуса УЦ

1.5. Предусматривающие уточнение порядка обезличивания персональных данных, условий и порядка их использования, порядка получения согласия и обеспечения соблюдения прав и интересов граждан, уточнение ответственности за ненадлежащие обработку и безопасность персональных данных

1.7. Предусматривающие определение состава сведений, составляющих соответственно банковскую тайну, тайну связи, врачебную тайну, коммерческую тайну и иные виды тайн, и порядка их передачи третьим лицам

План мероприятий программы "Цифровая экономика" по реформированию нормативно-правового регулирования (утвержден 18.12.2017 прав.комиссией по использованию ИТ для улучшения качества жизни ...)

Нарушение ИБ медицинских информационных (МИС) и технологических систем ->

- утечка конфиденциальной информации
- потеря / искажение данных, медицинских документов (ЭД, ЭМК)
- нарушение работоспособности (отказ), несанкционированное изменение режима работы медицинской техники -> **проблема киберзащищенности медицинской техники !!**

-> недоступность мед. помощи -> угроза жизни и здоровью граждан

Цифровая медицинская техника и МИС медицинской организации – объекты **критической информационной инфраструктуры** (КИИ) **!!**

Субъекты КИИ – гос.органы, гос. учреждения, российские юридические лица и(или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат объекты КИИ, функционирующие в сфере здравоохранения, науки, транспорта, энергетики *etc* = **учредитель (владелец) организации**

Компьютерный инцидент – факт нарушения и(или) прекращения функционирования объекта КИИ и(или) нарушения безопасности обрабатываемой информации

[закон № 187-ФЗ]

- Создание **комиссии по категорированию** объектов КИИ
- Выявление **критических процессов**, использующих объекты КИИ
  перечень процессов -> перечень объектов КИИ
- Утверждение субъектом **перечня объектов КИИ** -> ФСТЭК
  Согласование перечня с госорганом, выполняющим функции по нормативно-правовомоу регулированию в установленной сфере в части подведомственных субъектов КИИ (п.15 ПП-127) – с минздравом **?!**
- Присвоение категории объектам КИИ – **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: $T < 6$
- Создание системы безопасности и обеспечение функционирования объектов КИИ, подключение к ГосСОПКА, уведомление ФСБ об инцидентах *etc*

www.kmiac.ru – МИАЦ Красноярского края
www. www.brkmed.ru/category/miac/ – МИАЦ Брянской обл.
www.miac.nnov.ru – МИАЦ Нижегороской обл.

Субъект КИИ обязан:

- соблюдать установленные требования по обеспечению безопасности значимых объектов КИИ
- обеспечивать выполнение порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты
- незамедлительно информировать ФСБ об инцидентах
- реагировать на компьютерные инциденты и принимать меры по ликвидации последствий компьютерных атак
- оказывать содействие должностным лицам ФСБ в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения инцидентов
- обеспечивать беспрепятственный доступ должностным лицам ФСТЭК к значимым объектам КИИ
- выполнять предписания должностных лиц ФСТЭК и ФСБ по устранению выявленных нарушений

[ст. 9 закона № 187-ФЗ]

Субъект КИИ имеет право:

- получать от ФСТЭК информацию, необходимую для обеспечения безопасности "своих" значимых объектов КИИ
- получать от ФСБ информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения
- с согласия ФСБ за свой счет приобретать, арендовать, устанавливать и обслуживать средства обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты
- разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта КИИ

Наверное, это все-таки его обязанность ?!

[ст. 9 закона № 187-ФЗ]

Статья 274.1 УК РФ, часть 3 – нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой информации, содержащейся в КИИ, или объектах КИИ, либо правил доступа к указанным информации и(или) обектам – до 6 лет

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

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

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

Обработка данных персонифицированного учета лиц, которым оказывается медицинская помощь <...> осуществляется в ЕГИСЗ в обезличенном виде [ст. 91.1 закона № 323-ФЗ]

Порядок обезличивания сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, осмотры и освидетельствования, приказ Минздрава России от 14.06.2018 № 341н (только в ЕГИСЗ...)

Передача персональных данных пациента МО -> ЕГИСЗ только с его согласия (п. 44 ПП-555) – процедуры, форма согласия **?!**

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне ИС перс. данных, № 512 от 06.07.2008

Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, № 687 от 15.09.2008

Требования к защите персональных данных при их обработке в информационных системах персональных данных, № 1119 от 01.11.2012

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

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

Приказы ФСТЭК от 11.02.2013 № 17, от 18.02.2013 № 21, ФСТЭК и ФСБ от 31.08.2010 № 416/489, ГОСТ Р 51583-2014

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**

Указы Президента Российской Федерации

Об утверждении перечня сведений конфиденциального характера, № 188 от 06.03.1997 (ред. от 13.07.2015)

О некоторых вопросах информационной безопасности РФ. Порядок подключения информационных систем и телекоммуникационных сетей к сети Интернет и размещения (публикации) в ней информации через российский государственный сегмент Интернет, № 260 от 22.05.2015

О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (**ГосСОПКА**), № 31с от 15.01.2013, № 620 от 22.12.2017

Стратегия национальной безопасности РФ, № 683 от 31.12.2015

Доктрина информационной безопасности РФ, № 546 от 05.12.2016

Национальный координационный центр по компьютерным инцидентам, приказ ФСБ от 24.07.2018 № 366 – `www.gov-cert.ru`

FinCERT – Центробанк России, www.cbr.ru [CSIRT, CERT]

General Data Protection Regulation – GDPR Directive EU 2016/679, 27 April 2016

Network and Information Security – NIS Directive EU 2016/1148, 6 July 2016

– с 25 мая 2018, тестирование на ИБ всех клиник *etc*