9 – 10 июня 2020

ИТМ Сибирь+

Виртуальная конференция

Кибербезопасность как осознанная необходимость

Обеспечение кибербезопасности в здравоохранении: обзор последних нормативных актов

Сеченовский Университет

ВЫСШАЯ ШКОЛА УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ

www.hsha.ru

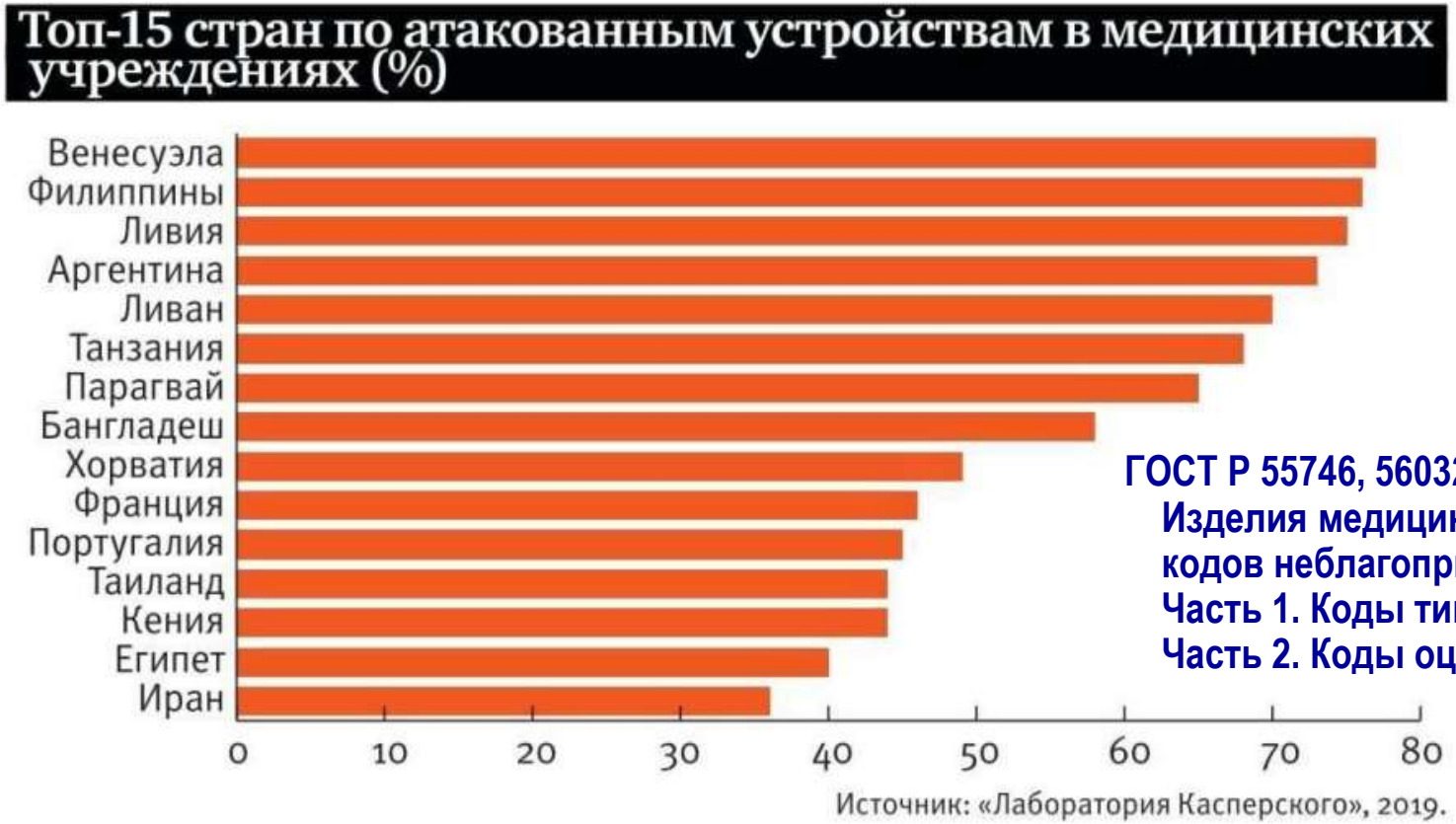
Столбов Андрей Павлович

10 июня 2020 г.

960.ИТМСиб.ОКБ

Главврач Тюменского федерального центра нейрохирургии А. Суфианов сообщил о хакерской атаке во время операции на головном мозге 13-летней девочки, в результате которой все приборы, сопровождавшие операцию, были отключены. Врачи сумели довести операцию до конца фактически без показаний приборов и снимков на мониторах.

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



ГОСТ Р 55746, 56032 / ISO/TS 19218-1,2
Изделия медицинские. Структура кодов неблагоприятных событий.
Часть 1. Коды типов событий.
Часть 2. Коды оценки

Взлом ЕПГУ – январь, декабрь 2019 (Kaspersky Lab, habr.com)

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

Утечки конфиденциальной информации за 2019 (InfoWatch, 28.05.2020)

Рост утечек за 2019/18: в мире – на 22.5%, в РФ – на 56%, 75% – персданные

Утечки персданных в РФ в 2019 (умышленные – 56%, в мире – 60.2%):

23.6%	госорганы	**23.5%**	телеком
21.6%	медицинские организации (2018 – 8.5%)	**10.2%**	образование
8.1%	банки и платежные системы	**6.8%**	торговля
61.6%	через браузер и облачные сервисы		
16.4%	через электронную почту	**13.4%**	через "бумагу"
3.8%	"прослушка"	**2.2%**	через "флешки"

78.4% инцидентов из-за низкой организации, незнания и халатности

Рост нарушений ИБ в банках в 5 раз, всего > 1.1 тыс (ЦБ России, 19.02.2020)

90% веб-приложений подвержены угрозе атак (Positive Technologies, 13.02.2020)

Сокрытие информации об инцидентах нарушения ИБ !!

Сложность системы защиты и затраты на ИБ стали сопоставимы со сложностью и затратами на решение прикладных задач !!

О едином федеральном информационном регистре, содержащем сведения о населении РФ, № 168-ФЗ от 08.06.2020 – с 01.01.2026 в полном объеме

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

- ред. от 01.05.2019 № 90-ФЗ – обеспечение устойчивости российского сегмента сети Интернет + идентификация сайтов в сети Интернет
- ред. от 03.04.2020 № 105-ФЗ – дистанционная торговля безрецептурными лекарственными препаратами

О персональных данных, № 152-ФЗ от 27.07.2006

- ред. от 24.04.2020 № 123-ФЗ – эксперимент по использованию ИИ в г. Москве с 01.07.2020 на 5 лет – использование обезличенных данных о состоянии здоровья

Об основах охраны здоровья граждан в РФ, № 323-ФЗ от 21.11.2011

- ред. от 01.01.2020 № 93-ФЗ – ст. 13 Врачебная тайна – доступ должностных лиц ФСИН без согласия пациента (наркомана)

О защите прав отребителей, № 2300-1 от 07.02.1992 – ред. от 02.12.2019 № 425-ФЗ

- ред. от 24.04.2020 № 144-ФЗ – предустановка российского ПО с 01.01.2021

О безопасности критической информационной инфраструктуры РФ, № 187-ФЗ от 26.07.2017

Об электронной подписи, № 63-ФЗ от 06.04.2011 (ред. от 27.12.2019, от 08.06.2020)

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, – приказ ФСТЭК от 11.02.2013 № 17 - в ред. приказа № 61 от 17.04.2020

- **Перенос срока применения требований по уровням доверия к сертифицированным СЗИ в ГИС на 01.01.2021 – раньше было 01.06.2020**

Информационное сообщение ФСТЭК от 20.01.2020 № 240/24/250

- **Исключение из реестра сертифицированных СЗИ с 01.06.2020 операционных систем MS Windows 7 и MS Windows Server 2008 R2**
- **Переход на ОС с гарантийной и(или) технической поддержкой – требования приказа ФСТЭК от 25.12.2017 № 239 для объектов КИИ**

проблемы для цифровой медицинской техники !?

Информационное сообщение ФСТЭК от 20.03.2020 № 240/84/389

- **Рекомендации по обеспечению безопасности объектов КИИ при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов КИИ -> запрет предоставления удаленного доступа ["из дома"] для администрирования и управления режимами работы цифровой медицинской техники, являющейся значимыми объектами КИИ !!**

Перечень нормативных правовых актов или их отдельных частей, оценка соблюдения которых является предметом государственного контроля в области обеспечения безопасности значимых объектов КИИ,
– приказ ФСТЭК от 06.07.2019 № 135 – перечень в ред. от 06.11.2019

Информационное сообщение ФСТЭК от 17.04.2020 № 240/84/611 о предоставлении перечней объектов КИИ, подлежащих категорированию, и направлении сведений о результатах категорирования + форма перечня

- для государственных учреждений – категорирование до 01.09.2020 !! (постановление Правительства РФ от 13.04.2019 № 452)

Информационное сообщение ФСТЭК от 09.04.2020 № 240/22/1534 о проекте "Методики определения угроз безопасности информации в информационных системах" – сбор замечаний до 30.04.2020

- антропогенные угрозы безопасности информации в ИСПДн, ИС (МИС) / АС, АСУ (ЦМТ) и ИТКС, в том числе отнесенных к объектам КИИ
- в случае принятия – отмена "Методики определения актуальных угроз безопасности ПДн при их обработке в ИСПДн" (2008) и "Методики определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры" (2007)

Требования по обеспечению безопасности значимых объектов КИИ, приказ ФСТЭК от 25.12.2017 № 239 – проект изменений от 06.02.2020 !!

- возможность удаленного доступа к ПО, ТС и СЗИ для обновления и управления только "дочерним" организациям субъекта КИИ (> 20% капитала) – если это невозможно -> принимать дополнительные меры безопасности
- определение термина "модернизация" – изменение архитектуры значимого объекта КИИ, в том числе подсистемы его безопасности по отдельному ТЗ
- требования к процессам оценки соответствия СЗИ + соответствие СЗИ, не встроенных в системное или прикладное ПО, уровню доверия ≥ 6
- размещение программно-аппаратных средств объектов КИИ не только 1-ой, но и 2-ой категории значимости на территории РФ
- требования по безопасной разработке и выявлению уязвимостей и НДВ в прикладном ПО !!

  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)

ГОСТ Р 58412-2019 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности при разработке ПО – с 01.11.2019

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

Национальный координационный центр по компьютерным инцидентам

www.cert.gov.ru – приказ ФСБ России от 24.07.2018 № 366

Электронная почта для сообщений о компьютерных инцидентах

incident@cert.gov.ru

Информационные сообщения НКЦКИ

- от 09.12.2019 – Состав технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, и форматы представления информации о компьютерных инцидентах -> уведомления (кодированные по номенклатурам)
  - о компьютерном инциденте / о признаке компьютерного инцидента
  - о компьютерной атаке
  - об уязвимости / о признаке уязвимости
- от 20.03.2020 – Об угрозах безопасности информации, связанных с пандемией коронавируса (COVID-19)
- Бюллетени о уязвимостях – https://safe-surf.ru/specialists/bulletins-nkcki/

www.bdu.fstec.ru на 05.06.2020: угроз – 217, уязвимостей – 27085

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

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

Присвоение категории объектам КИИ – критерии

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

III-я: 1 ≤ Nч ≤ 50; II-ая: 50 < Nч ≤ 500; I-ая: Nч > 500

Nч – расчет на основе статистических данных в ф.№ 30 и среднего времени восстановления после компьютерного инцидента **!?**

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

III-я: 12 < Тн < 24; II-ая: 6 < Тн < 12; I-ая: Тн < 6

Тн – из регламентов предоставления государственных услуг **!?**

Рекомендации по проведению процесса категорирования объектов критической информационной инфраструктуры учреждений сферы здравоохранения Российской Федерации. Методический документ. – ЦНИИОИЗ. Центр компетенции по цифровой трансформации в сфере здравоохранения. – ред. от 26.03.2020 (ПРОЕКТ)

Правила подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры, – постановление Правительства РФ от 08.06.2019 № 743 – с 01.01.2020

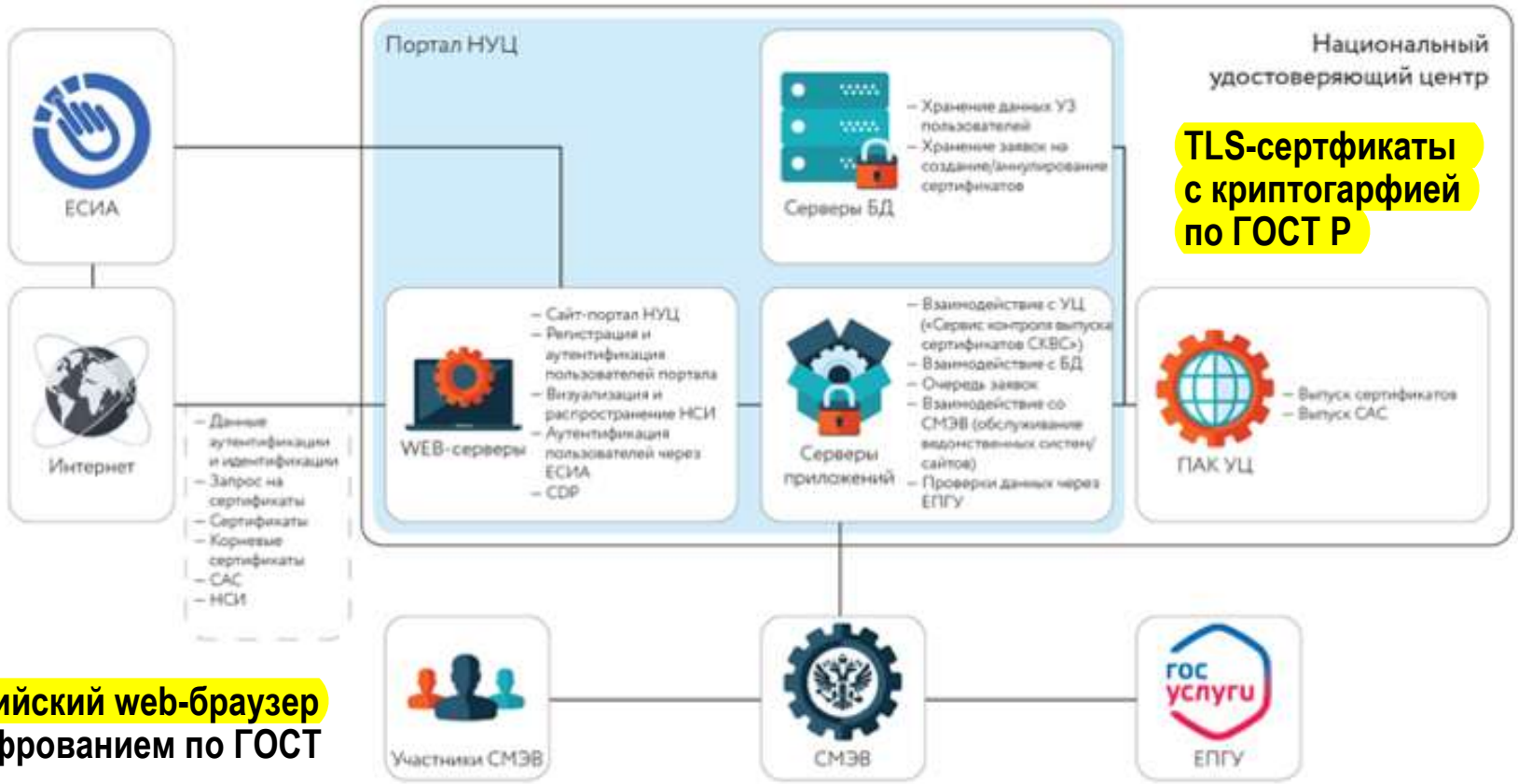
Порядок согласования ФСТЭК подключения значимого объекта критической информационной инфраструктуры РФ к сети связи общего пользования – в части достаточности применяемых СЗИ – проект приказа ФСТЭК – 30.04.2020

21.05.2020 – проекты указа Президента РФ, постановлений Правительства РФ и приказов Минкомсвязи России о переходе значимых объектов КИИ на использование

- российского и евразийского программного обеспечения – до 01.01.2021
- российского оборудования – до 01.01.2022
- Правительству РФ до 01.09.2020 – утвердить требования к ПО и оборудованию и порядок перехода на его преимущественное использование на объектах КИИ

ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения – с 01.05.2020

Национальный удостоверяющий центр



Российский web-браузер с шифрованием по ГОСТ

Разработка – до 30.04.2020 (Инфотекс Траст), ввод в действие – конец 2020

Р 1323565.1.020-2018. Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2) – действуют с 01.02.2019

Благодарю за внимание !
Вопросы ?

Столбов Андрей Павлович

ap100Lbov@mail.ru

www.hsha.ru

Вестник Росздравнадзора, 2020, № 3

Сеченовский Университет

ВЫСШАЯ
ШКОЛА
УПРАВЛЕНИЯ
ЗДРАВООХРАНЕНИЕМ

ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения. – с 01.05.2020

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 29161-2019 Информационные технологии. Структура данных. Уникальная идентификация для интернета вещей

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

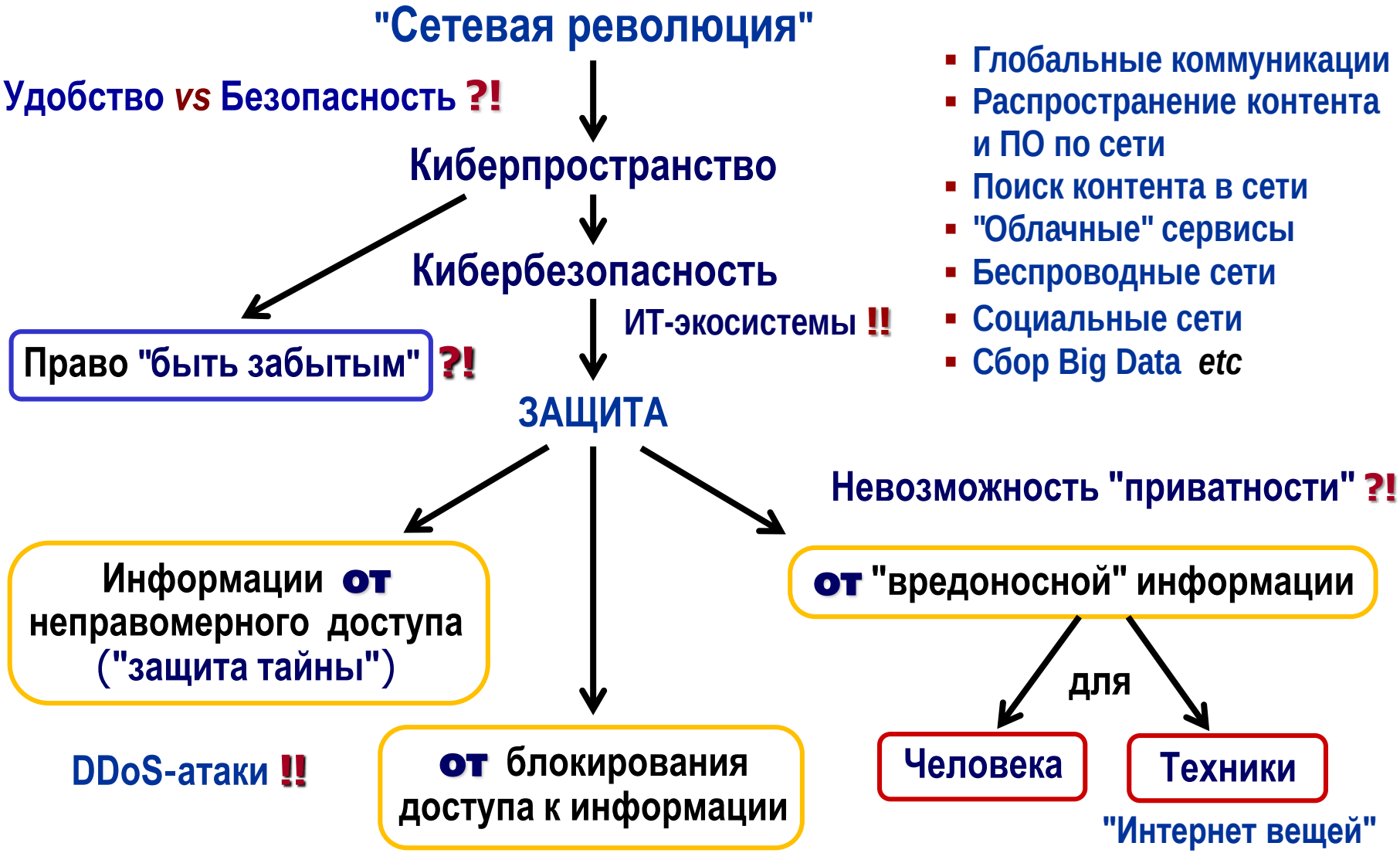
ГОСТ Р ИСО 27799-2015 Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002

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



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

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 (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

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

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

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]

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 ФИЭМК)

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