ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕДИЦИНЕ

ИТМ 2022

Обеспечение кибербезопасности субъектов критической информационной инфраструктуры в здравоохранении. Нормативное регулирование и практика применения

Обеспечение кибербезопасности в здравоохранении: обзор актуальных нормативных документов

Сеченовский Университет

ВЫСШАЯ ШКОЛА УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ

www.hsha.ru

Столбов Андрей Павлович

14 октября 2022 г.

О персональных данных, № 152-ФЗ от 27.07.2006 - в ред. от 14.07.2022 № 266-ФЗ

с 1 сентября 2022 !!

- **установлен срок ответа оператора субъекту персональных данных и Роскомназору (по его запросу) – до 10 рабочих дней** (возможно продление до 15 дней) **(ст. 14, ст. 20)**
- **возможность автоматизированной обработки персданных без уведомления Роскомнадзора (РКН) только операторами ГИС, созданных в целях защиты безопасности государства и общественного порядка, а также в случаях, предусмотренных законодательством о транспортной безопасности (ст. 22)**
- **расширен состав сведений предоставляемых в РКН в уведомлении – для каждой цели и категории субъектов *etc* (часть 3.1 ст. 22)**
- **установлен срок уведомления РКН об изменениях – до 15-го числа следующего месяца, в котором произошли изменения (часть 7 ст. 22)**
- **при обнаружении факта утечки персданных оператор обязан в течение 24 часов уведомить об этом и о возможных причинах РКН, а в течение 72 часов уведомить РКН о результатах внутреннего расследования (часть 3.1 ст. 21)**
- **обязанность оператора взаимодействовать с ГосСОПКА и информировать ФСБ об инцидентах, приведших к утечке персданных – ФСБ затем сообщает об этом в РКН (части 12-14 ст. 19)**
- **Роскомнадзор ведет реестр учета инцидентов в области персданных и передает эти сведения в ФСБ (части 10, 11 ст. 23)**
- **обязанность оператора уведомлять РКН о трансграничной передаче персданных (ст. 12) – с 1 марта 2023 !!**

электронные формы уведомлений – на сайте РКН **www.rkn.gov.ru**

Указы Президента РФ: от 15.01.2013 № 31с (ГосСОПКА), от 30.03.2022 № 166, от 01.05.2022 № 250

Постановления Правительства РФ

- № 1119 от 01.11.2012 \ ИСПДн
- № 162 от 17.02.2018 \ КН КИИ
- № 1046 от 29.06.2021 \ КН ОПДн
- № 1272 от 15.07.2022
- № 676 от 06.07.2015 \ ГИС
- № 127* от 08.02.2018 \ КИИ ред. от 19.08.22 № 1463*
- № 211 от 21.03.2012 \ ПДн
- № 1066, № 1067 от 15.06.2022, № 1089 от 16.06.2022 \ БМС
- № 1478 от 27.08.2022 \ ПО
- № 605 от 06.04.2022 \ НУЦ
- № 875 от 14.05.2022 \ 2ФА
- № 860 от 13.05.2022 \ ЭУЗ

Приказы и методические документы ФСТЭК России

- № 17 от 11.02.2013 \ ГИС
- № 235 от 21.12.2017 \ КИИ
- № 236 от 22.12.2017 \ ф.КИИ
- № 77 от 29.04.2021 \ аттестация ГИС
- № 21 от 18.02.2013 \ ИСПДн, меры
- № 277* от 06.12.2017 \ Реестр ОКИИ
- № 239 от 25.12.2017 \ КИИ, меры
- № 75 от 28.05.2020 \ КИИ, сети связи
- Меры защиты информации в государственных ИС – 11.02.2014
- Методика оценки угроз безопасности информации – 05.02.2021
- О мерах по повышению защищенности информационной инфраструктуры – 24.03.2022

* МЗ РФ – мониторинг предоставления сведений о ОбКИИ в отрасли с привлечением подвед. орг-ций для проверки их достоверности

Приказы и методические документы ФСБ России

- № 378 от 10.07.2014 \ ИСПДн
- № 282* от 19.06.2019 \ уведомл. инц.
- № 367 от 24.07.2018 \ ГосСОПКА
- № 366 от 24.07.2018 \ НКЦКИ
- № 368 от 24.07.2018 \ КИИ - Обмен и получение информации
- № 196 от 06.05.2019, № 281 от 19.06.2019 \ СрОПЛКА
- Рекомендации по минимизации возможных угроз информационной безопасности – НКЦКИ, 29.03.2022

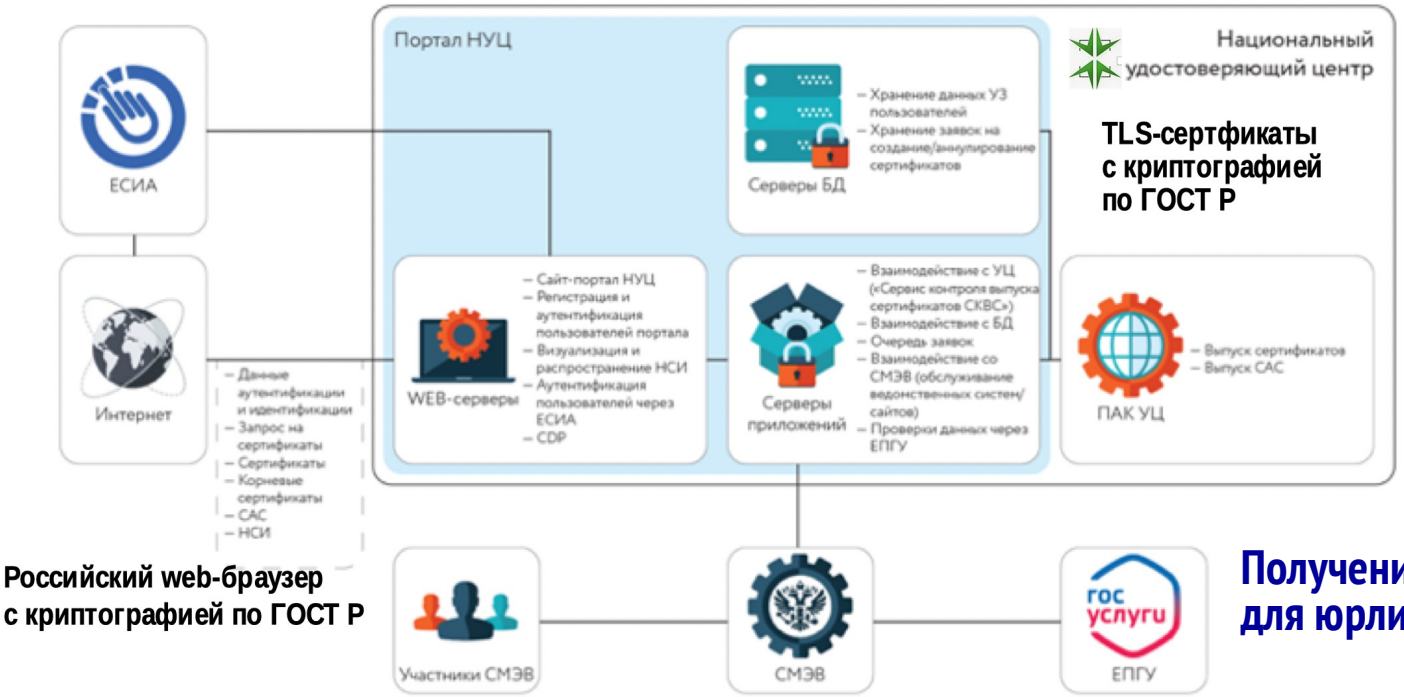
Приказы и методические документы Минцифры России

- № 186 от 10.03.2022
- Типовое ТЗ <...> по оценке уровня защищенности информационной инфраструктуры, 03.06.2022

Приказы и документы Роскомнадзора

- № 996 от 05.09.2013 \ обезличивание
- № 272 от 18.10.2016 (ред. от 17.07.2020) \ Перечень НПА
- № 253 от 24.12.2021 \ Проверочный лист ОПДн
- Методрекомендации по применению приказа № 996, утв. 13.12.2013

Национальный удостоверяющий центр НУЦ https://nucrf.ru



ЕПГУ – можно скачать сертификаты, Яндекс и Атом – Минцифры РФ, 19.09.2022

Постановление Правительства РФ от 06.04.2022 № 605

Получение TLS-сертификатов для юрлиц на ЕПГУ – gosuslugi.ru/tls !!

Минздрав России – с 06.04.2022 в ЕГИСЗ будут применяться сертификаты, выпущенные НУЦ !!

Инструкции по настройке доверия сертификатам в браузерах (кроме "Яндекса" и "Атома") – https://portal.egisz.rosminzdrav.ru/news/701, 02.04.2022

Проверка корректности настройки – https://fias.egisz.rosminzdrav.ru/

О реализации пилотного проекта по использованию российских криптографических алгоритмов и средств шифрования в государственных информационных системах (15.07.2020 - 01.03.2021). – постановление Правительства от 30.06.2020 № 963

Р 1323565.1.020-2018. Рекомендации по стандартизации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)

Постановления Правительства Российской Федерации

№ 1272 от 15.07.2022

- **Типовое положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации)** \ высшее образование или ПП (> 360 ч.) по ИБ
- **Типовое положение о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)**

№ 1478 от 22.08.2022

- **Требования к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах КИИ** \ в реестре ПО РФ, ЕАЭС, сертификат для СЗИ
- **Правила согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования** <...> **на значимых объектах КИИ** \ согласование с Минздравом России
- **Правила перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, органов государственной власти, заказчиков** <...> **на принадлежащих им значимых объектах КИИ** \ Минздрав России – отраслевой План с разбивкой по классам ПО и Перечень мероприятий по организационному и нормативному обеспечению процесса перехода (согласованы межведомственной комиссией)

Постановления Правительства РФ

- **№ 140 от 09.02.2022 –** Положение о ЕГИСЗ
- **№ 447 от 12.04.2018 –** Правила взаимодействия иных ИС <...> с ИС в сфере здравоохранения и медицинскими организациями

Концепция информационной безопасности в сфере здравоохранения.

– утверждена президиумом Правительственной комиссии по цифровому развитию, использованию ИТ <...>, протокол № 7 от 10.03.2022, 85 с., опубликована 22.06.2022

Отраслевой **Центр информационной безопасности и импортозамещения ПО** - на базе ЦНИИОИЗ

Приказы и методические документы Минздрава России

- **№ 911н от 24.12.2018 –** Требования к ГИС в сфере здравоохранения субъектов РФ, МИС медорганизаций, ИС фармацевтических организаций
- **№ 205н от 25.03.2022 –** Типовое положение о МИАЦ
- **№ 341н от 14.06.2018 –** Порядок обезличивания сведений о лицах, которым оказывается медицинская помощь, в отношении которых проводятся медицинские экспертизы, осмотры и освидетельствования \ МО -> ФИЭМК
- **Методические рекомендации по категорированию объектов КИИ сферы здравоохранения. – 05.04.2021,** ЦНИИОИЗ, 175 с.
- **Методические рекомендации по формированию службы информационных технологий в медицинских организациях. – 04.03.2022,** ЦНИИОИЗ, 61 с.

Письмо Росздравнадзора от 08.04.2022 № 01и-376/22 о рекомендациях по эксплуатации и техническому обслуживанию медицинских изделий.

Кибербезопасность цифровой медицинской техники (ЦМТ)

- отсутствие нормативных требований к классам киберзащищенности ЦМТ, принадлежностям и комплектущим изделиям в составе ЦМТ
- низкая защищенность ЦМТ – отсутствие в составе ЦМТ средств защиты информации (СЗИ), соответствующих требованиям, принятым в РФ
- необходимость подключения ЦМТ к удаленной ИС сервисной организации по каналу связи -> риск несанкционированого доступа в ИС медицинской организации
- возможные коллизии с настройками СЗИ после обновления ПО в составе ЦМТ-> риски несанкционированного кибервоздействия на ЦМТ и ИС медорганизации
- использование в составе ЦМТ средств вычислительной техники с "нестандартной" или уже не поддерживаемой производителем операционной системой -> возможная несовместимость ПО с сертифицированными СЗИ
- необходимость разработки модели угроз безопасности ЦМТ в конкретных условиях применения – с учетом конфигурации ЛИС \ РИС \ МИС *etc*
- необходимость оценки \ проверки киберзащищенности при государственной регистрации ЦМТ как медицинского изделия **!!**

В 2019 г. были атакованы 19% цифровых медизделий в мире. В 2021 г. – выявлены 18 критических уязвимостей в носимых медицинских изделиях.

54% медорганизаций в РФ используют медтехнику с устаревшими ОС, вследствие чего произошли 32% утечек данных и DDoS-атак и 30% атак "вымогателей".

[Kaspersky Lab, 8 декабря 2021]

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

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

ГОСТ Р 57301-2016 /ISO/TS 14441:2013 **Требования защиты и конфиденциальности систем ведения ЭМК (при оценке соответствия).**

ГОСТ Р 59547-2021 Мониторинг информационной безопасности. Общие положения

ГОСТ Р ИСО/МЭК 27000, 27001, 27002, 27003, 27004, 27014, 27017, 27021-2021 Менеджмент информационной безопасности

ГОСТ Р ИСО/МЭК 27034-2, -3, -6-2021 Безопасность приложений

ГОСТ Р 59383-2021 Основы управления доступом

ГОСТ Р 59407-2021 Базовая архитектура защиты персональных данных

ГОСТ Р 59503-2021 Экономика информационной безопасности организации

ГОСТ Р 59548-2022 Регистрация событий безопасности. Требования к регистрируемой информации

ГОСТ 34.602-2020 Техническое задание на создание автоматизированной системы

ГОСТ Р 59792-2021 Виды испытаний автоматизированных систем

ГОСТ Р 59795-2021 Автоматизированные системы. Требования к содержанию документов

Приказ Минтруда РФ от 09.08.2022 № 474н – Профстандарт **"Специалист по технической защите информации"**

U.S. Department of Health & Human Services, 28.12.2018 www.hhs.gov

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

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 (ed. 18.10.2018)

Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. Guidance for Industry, January 2005 (ed. 02.02.2018)

FDA CDRH and Medical Device Cybersecurity: Response to NIST Regarding President's Executive Order on Improving the of the Federal Government (EO 14028), 26.05.2021

Best Practices for Communicating Cybersecurity Vulnerabilities to Patients, 01.10.2021

Playbook for Threat Modeling Medical Devices, 30.11.2021 www.fda.gov

MDCG 2019-16 – Guidance on Cybersecurity for medical devices. European Commission, 07.01.2020 (ed. 22.06.2020) www.ec.europa.eu

IMDRF/CYBER WG/N 60 Principles and Practices for Medical Device Cybersecurity. – 20.04.2020 www.imdrf.org

Cloud Security for Healthcare Services. - The European Union Agency for Cybersecurity (ENISA), 18.01.2021

Data Pseudonymisation: Advanced Techniques and Use Cases. - ENISA, 28.01.2021

Deploying Pseudonymisation Techniques. - ENISA, 24.03.2022 www.enisa.europa.eu

Благодарю за внимание!

Столбов Андрей Павлович

stolbov_a_p@staff.sechenov.ru

ap100Lbov@mail.ru

Сеченовский Университет
ВЫСШАЯ ШКОЛА УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ
www.hsha.ru

Статья 10. Специальные категории персональных данных

<...>

2.1. Обработка персональных данных, касающихся состояния здоровья, полученных в результате обезличивания персональных данных, допускается в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом от 24.04. 2020 № 123-ФЗ "О проведении эксперимента по установлению специального регулирования в целях <...> разработки и внедрения технологий искусственного интеллекта в <...> г. Москве <...> и Федеральным законом от 31.07. 2020 № 258-ФЗ "Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации", в порядке и на условиях, которые предусмотрены указанными федеральными законами.

[закон № 152-ФЗ в ред. закона № 331-ФЗ от 02.07.2021; см. также п. 9.1 части 1 ст. 6]

Конфиденциальность – Степень обезличивания – Риск де-обезличивания !?

Согласие пациента на обезличивание и использование обезличенных данных о состоянии его здоровья в определенных целях ?!

По достижении целей обработки персональные данные должны быть уничтожены либо обезличены, если срок их хранения не установлен федеральным законом или договором, по которому осуществляется обработка персональных данных [ч. 7 ст. 5 закона № 152-ФЗ]

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]

Передача персональных данных пациента МО -> ЕГИСЗ только с его согласия (п. 49 постановления № 140) – процедуры оформления, форма согласия ?!

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 для ФИЭМК

Приказ РЗН от 11.02.2022 № 973, п. 117 пр. № 1 – проверка соблюдения порядка обезличивания сведений при передаче из МИС МО в ФИЭМК \ как это будут проверять **?**

Предложения

- **Разработать базовую отраслевую интегральную модель угроз информационной безопасности КИИ (медтехника + МИС) + ИСПДн и комплект типовых организационно-распорядительных и методических документов по обеспечению кибербезопасности в медорганизациях**
- **Разработать классификацию цифровой медицинской техники по уровням киберзащищенности (классы киберзащищенности) и типовые методики оценки (определения) киберзащищенности ЦМТ**
- **Предусмотреть в "дорожных картах" по созданию "Единого цифрового контура" мероприятия по повышению осведомленности руководителей и работников медицинских организаций и МИАЦ в вопросах обеспечения кибербезопасности, госзакупок ИТ-продукции *etc***
- **Проработать вопрос о применении технологии LPS /TENS (Lightweight Portable Security / Trusted End Node Security) на основе LiveUSB для создания VPN-клиентов, защищенных АРМ медработников, работы с электронными документами, телемедицины *etc***

– опыт органов власти Ленобласти [CNews, 3 декабря 2021]

Столбов А.П. О кибербезопасности медицинской деятельности. Вестник Росздравнадзора, 2020;(3):44-52.