MedSoft - 2024

Обеспечение кибербезопасности в здравоохранении:
нормативные требования, проблемы и решения

Кибербезопасность медицинской деятельности: обзор новых нормативных документов

Сеченовский Университет
ВЫСШАЯ ШКОЛА УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ
www.hsha.ru

Столбов Андрей Павлович

5 апреля 2024 г.

Указы Президента РФ

О представлении сведений, содержащихся в документах, удостоверяющих личность гражданина РФ, с использованием информационных технологий.
– **№ 695** от 18.09.2023
- с помощью мобильного приложения ЕПГУ
- перечень случаев – Правительство РФ по согласованию с ФСБ

О полномочиях и функциях ФСТЭК России,
– **№ 846** от 08.11.2023
- оперативно информирует ФОИВ, ОИВ субъектов РФ, органы местного самоуправления и организации об угрозах ИБ и уязвимостях ИС и иных объектов КИИ, а также о мерах по технической защите от этих угроз и уязвимостей
- обеспечивает создание и функционирования АИС для управления деятельностью по технической защите информации и обеспечению безопасности значимых объектов КИИ
- осуществляет централизованный учет ИС и иных объектов КИИ по отраслям экономики, а также мониторинг текущего состояния защиты и безопасности значимых объектов КИИ

Проекты указов

Об утверждении Положения о государственной системе защиты информации в РФ. – 23.01.2023

О государственной системе защиты информации в РФ от иностранных технических разведок и от ее утечки по техническим каналам.
– постановление Правительства РФ от 15.09.1993 № 912-51

О внесении изменений в Указ Президента РФ от 1 мая 2022 г. № 250 … – 20,06.2023
- определить порядок аккредитации центров ГосСОПКА, требования к центрам и порядок контроля за их деятельностью (ФСБ России)

Обезличивание персональных данных
- Законопроект № 992331-7 от 21.07.2020
- Поручение Президента РФ от 08.09.2023
  – принять закон до 15.12.2023

Федеральный закон № 584-ФЗ от 29.12.2022

– **с 01.03.2023** – части 8 – 10 ст. 10 закона № 149-ФЗ

Запрет на использование иностранных мессенджеров

- госкомпаниями; унитарными предприятиями; публично-правовыми компаниями; организациями, в которых доля участия РФ, субъекта РФ или муниципального образования превышает 50%; страховыми организациями – **для передачи**:
  - **персональных данных** граждан РФ
  - информации при предоставлении государственных и муниципальных услуг
  - информации при реализации товаров, работ и услуг
- всеми операторами персональных данных – **для передачи** информации при осуществлении платежей

Иностранные мессенджеры:

- Discord
- Microsoft Teams
- **Skype**
- Snapchat
- Viber
- **Telegram**
- Threema
- WeChat
- **WhatsApp**

Приказ Роскомнадзора от 21.02.2023 № 22
https://rkn.gov.ru/news/rsoc/news74672

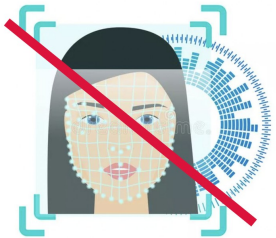
За нарушение – штраф
по ст. 13.11.2 КоАП РФ
(закон № 277-ФЗ от 24.06.2023)

- на должностных лиц
  – от 30 до 50 тыс. руб
- на юридических лиц
  – от 100 до 700 тыс. руб

Биометрическая аутентификация

не допускается при: – с **01.06.2023** ‼

- оказании медицинской помощи
- отпуске лекарственного препарата по рецепту
- получении информированного добровольного согласия на медицинское вмешательство или отказ от него
- получении медицинских документов (копий)
- проведении дистанционных медосмотров работников и контроля за их состоянием
- предоставлении государственных и муниципальных услуг
- предоставлении доступа к ГИС



Постановления Правительства РФ

Перечень случаев, при которых аутентификация с использованием ИС организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, **не допускается** [...] и при которых допускается [...]
– **№ 815** от 25.05.2023

О внесении изменений в некоторые акты Правительства РФ.
– **№ 341** от 20.03.2024
-> регистрация гражданина в гостинице, **санатории**, **медорганизации** [...] на основе сведений из **ЕСИА**, после идентификации и(или) аутентификации с использованием единой биометрической системы

Об осуществлении идентификации и(или) аутентификации физических лиц с использованием биометрических персональных данных [...]
– федеральный закон **№ 572-ФЗ** от 29.12.2022

Единая система биометрической идентификации (ЕБС) – интеграция с ЕСИА, возможность запрета (отказа) биометрической идентификации и аутентификации

Федеральный закон № 406-ФЗ от 31.07.2023

– изменения в законы № 149-ФЗ и № 126-ФЗ

- запрет регистрации пользователей на российских сайтах и ИС с помощью аккаунтов в иностранных ИС (gmail.com и т.п.)
- авторизация пользователей на российских сайтах и ИС при доступе к ним через Интернет – только с помощью:
  - номера мобильного телефона, ЕСИА, ЕБС,
  - иных российских ИС, соответствующих требованиям ИБ

  – с 01.12.2023 (ч. 10 ст. 8 закона № 149-ФЗ)
- уведомление Роскомнадзора о предоставлении вычислительной мощности для размещения информации в ИС, подключенной к сети Интернет

  – с 01.12.2023 (ст. 10.2-1 закона № 149-ФЗ)
- предоставление хостинга без включения в реестр Роскомнадзора запрещено

  – с 01.02.2024 (ч. 11 ст. 10.2-1 закона № 149-ФЗ)
- операторы ГИС, ИС государственных и муниципальных предприятий и учреждений должны использовать мощности провайдера хостинга, включенного в реестр, и не вправе использовать мощности, принадлежащие иностранным лицам

  – с 01.09.2024 (части 2.1-1, 2.4 ст. 13 закона № 149-ФЗ)

Постановления Правительства РФ

Правила формирования и ведения реестра провайдеров хостинга.
– **№ 2008** от 28.11.2023

Правила прохождения идентификации и(или) аутентификации лицами, обратившимися к провайдеру хостинга в целях получения вычисл. мощности для размещения информации в ИС, постоянно подключенной к Интернет.
– **№ 2022** от 29.11.2023

Приказы Минцифры России

Требования о защите информации при предоставлении вычисительной мощности для размещения информации в ИС, постоянно подключенной к сети Интернет. – **№ 936** от 01.11.2023

Перечень индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных.
– **№ 1187** от 15.11.2021 – в ред. приказа **№ 720** от 17.08.2023 (неверные сведения на сайте)

Законопроект № 581689-8 от 21.03.2024 г.

– о внесении изменений в федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации"

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Цели законопроекта

- обеспечение технологической независимости субъектов КИИ посредством перехода на преимущественное использование российского ПО, баз данных и радиоэлектронной продукции на объектах КИИ
- совершенствование механизма категорирования объектов КИИ путем наделения Правительства РФ полномочиями:
  - ✔ определять по каждой отрасли типы ИС, которые необходимо будет относить к значимым объектам КИИ с учётом отраслевых особенностей
  - ✔ устанавливать сроки перехода на российскую продукцию с учетом готовности отечественных решений
  - ✔ переход и соблюдение сроков будут контролироваться отраслевыми министерствами

Предполагается, что закон будет принят и вступит в силу с 1 марта 2025 г.

Постановления Правительства России (1)

Порядок перехода субъектов КИИ на преимущественное применение **доверенных** программно-аппаратных комплексов (ПАК) на принадлежащих им значимых объектах КИИ.
– **№ 1912** от 14.11.2023

- **доверенный ПАК** – соответствует всем следующим критериям:
  - сведения о нём содержатся в едином реестре российской радиоэлектронной продукции – **gisp.gov.ru** (см. постановление № 878)
  - ПО в составе ПАК должно быть зарегистрировано в реестре российского ПО или в реестре программ для ЭВМ и БД ЕАЭС (см. постановление № 1236)
  - если ПАК реализует функцию защиты информации, он должен иметь сертификат ФСТЭК и(или) ФСБ
- приобретение для значимых объектов КИИ только доверенных ПАК, за исключением случаев случаев отсутствия аналогов в РФ (подтверждение отсутствия аналогов – см. постановление № 1135)
  – с 1 сентября 2024 г. **!!**
- полный переход на доверенные ПАК – до 1 января 2030 г.

ПНСТ 905-2023 Критическая информационная инфраструктура. Доверенные программно-аппаратные комплексы. Термины и определения
– с 1 апреля 2024 г.

Импортозамещение

- **№ 1236** от 16.11.2015 – запрет на допуск ПО из иностранных государств для госзакупок (в ред. от 30.11.2023 № 2044)
- **№ 325** от 23.03.2017 – дополнительные требования к программам для ЭВМ и БД, включенным в реестр российского ПО (в ред. от 07.03.2018 № 234)
- **№ 1135** от 20.09.2017 – отнесение продукции к не имеющей аналогов в РФ (в ред. от 14.06.2023 № 980)
- **№ 1478** от 22.08.2022 – требования к ПО, в том числе в составе ПАК, на значимых объектах КИИ
- **№ 878** от 10.07.2019 – правила формирования и ведения единого реестра российской радиоэлектронной продукции (в ред. от 09.12.2023 № 2094)

Приказы Минцифры России

- **№ 21** от 18.01.2023 – методические рекомендации по переходу на российское ПО
- **№ 62** от 31.01.2023 (в ред. от 08.09.2023 № 792) – классификатор ПАК -> ПАК в сфере здравоохранения -> ПАК для проведения диагностики и лечения

Постановления Правительства России (2)

О внесении изменений в постановления Правительства РФ об использовании ЕСИА
– **№ 1739** от 19.10.2023 -> с 28.10.2023

- обязательная **двухфакторная аутентификация** для доступа к информации, содержащейся в государственных, муниципальных и иных ИС, в том числе через ЕПГУ
- способы дополнительной аутентификации: ◆ вход по биометрии; ◆ ввод одноразового кода из СМС или специального приложения
- право изменять способ дополнительной аутентификации с использованием личного кабинета на ЕПГУ

О продлении эксперимента по повышению уровня защищенности государственных ИС федеральных органов исполнительной власти и подведомственных им учреждений
– **№ 323** от 18.03.2024 -> до 31.12.2024 (было – до 30.03.2024)

- инвентаризация систем защиты информации
- выявление существующих недостатков (уязвимостей) в инфраструктурных, архитектурных и организационных решениях ГИС
- оценка уровня защищенности ГИС и их компонентов в рамках создания (развития) единой цифровой платформы "ГосТех"

Концепция информационной безопасности детей в Российской Федерации и признании утратившим силу распоряжения от 02.12.2015 № 2471-р.
– **№ 1105-р** от 28.04.2023

Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации.
– **№ 4088-р** от 22.12.2022

79% инцидентов – из-за низкой организации, незнания (**57**%) и халатности (**22**%) пользователей
[Kaspersky Lab, апрель 2023]

В целях реализации федерального проекта "Информационная безопасность" Ростандарт открыл доступ к ГОСТам в сфере ИБ, разработанным ТК 026 "Криптографическая защита информации" и ТК 362 "Защита информации" – 06.12.2023

rst.gov.ru/portal/gost//home/standarts/InformationSecurity

Приказы ФСБ России

Требования о защите информации, содержащейся в государственных ИС, с использованием шифровальных (криптографических) средств.
– **№ 524** от 24.10.2022

Об определении переходного периода, предусмотренного пп. "б" п. 5 Указа Президента РФ от 01.05.2022 № 250 ...
– **№ 543** от 01.11.2022

- госорганам и иным субъектам КИИ разрешается осуществлять мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты на основе заключенных с ФСБ (НКЦКИ) соглашений – в течение 3 лет – до 13 декабря 2025 г.

Порядок взаимодействия операторов с ГосСОПКА, включая информирование ФСБ о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.
– **№ 77** от 13.02.2023 -> **уведомление об инциденте**

- **субъект КИИ** -> НКЦКИ, об инциденте со значимым объектом КИИ – в течение 3 часов, с иным объектом КИИ – в течение 24 часов
- **не субъект КИИ** -> Роскомнадзор -> НКЦКИ – в течение 24 часов, результаты расследования – в течение 72 часов

Порядок осуществления мониторинга защищенности информационных ресурсов, принадлежащих ФОИВ, высшим органам государственной власти субъектов РФ, государственным фондам, госкомпаниям, иным организациям, [...] юридическим лицам, являющимся субъектами КИИ либо используемых ими. – **№ 213** от 11.05.2023

- только в отношении ресурсов, имеющих подключение к Интернет
- владелец ресурса должен направить в Центр мониторинга ФСБ информацию о доменных именах и внешних IP-адресах используемых ресурсов
- о всех изменениях или дополнениях доменных имен, внешних IP-адресов – информировать ФСБ в течение 7 р/дней
- оценка защищённости осуществляется на основании ежегодного плана с уведомлением не позднее чем за 14 календарных дней до начала проведения проверки

Приказы ФСТЭК России

Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования.
– приказ **№ 235** от 21.12.2017 (в ред. от 20.04.2023 № 69)

- возможность привлечения специалистов со средним профессиональным образованием по ИБ
- сокращены сроки переподготовки специалистов по ИБ с 5 до 3 лет
- обязательные компенсирующие меры при невозможности техподдержки СЗИ со стороны производителя

Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети. – **№ 44** от 07.03.2023

Требования по безопасности информации к системам управления базами данных. – **№ 64** от 14.04.2023

Методические документы ФСТЭК

Руководство по организации процесса управления уязвимостями в органе (организации). – утвержден 17.05.2023

Методика оценки показателя состояния защиты информации и обеспечения безопасности объектов КИИ (**проект**),
– информационное сообщение от 12.02.2024 № 240/91/688

Информационные сообщения ФСТЭК

О примерной программе профессиональной переподготовки "Информационная безопасность. Техническая защита конфиденциальной информации"
– от 19.07.2023 № 240/11/3462

О новых редакциях примерных программах профессиональной переподготовки и повышения квалификации специалистов в области противодействия иностранным техническим разведкам, технической защиты информации и обеспечения безопасности значимых объектов КИИ.
– от 19.07.2023 № 240/11/3463

Перечень организаций, осуществляющих образовательную деятельность, имеющих дополнительные профессиональные программы в области информационной безопасности (согласованы с ФСТЭК и ФСБ)
– fstec.ru/files/695/----/1315/----.odt

Документы Минздрава России

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в ИС ПДн, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Минздравом России.
– приказ **№ 340н** от 03.07.2023 – с 18.08.2023
bdu.fstec.ru – 222 угрозы, более 55720 уязвимостей

Методические рекомендации медицинским организациям по организации криптографической защиты каналов при взаимодействии в рамках ЕГИСЗ. – 31.08.2023, – 15 с.

Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере здравоохранения.
– утвержден Минздравом России 27.12.2023, согласован с ФСТЭК, опубликован 24.01.2024

Концепция информационной безопасности в сфере здравоохранения.
– утверждена Правительственной комиссией по цифровому развитию, протокол № 7 от 10.03.2022, опубликована 22.06.2022. – 85 с.

Рекомендации по эксплуатации и техническому обслуживанию цифровой медицинской техники в условиях санкций.
– Письмо Росздравнадзора от 08.04.2022 № 01и-376/22

Отраслевой **Центр информационной безопасности** и импортозамещения программного обеспечения (в ЦНИИОИЗ)

- разработка типовых локальных нормативных актов и организационно-распорядительных документов по защите информации организаций в сфере здравоохранения
- создание единой базы знаний типовых документов по защите информации в ИС в сфере здравоохранения
- создание библиотеки методических рекомендаций по реализации мер защиты информации
- оказание методической и практической помощи участникам системы обеспечения ИБ в здравоохранении
- взаимодействие с ФСТЭК и ФСБ России по вопросам обеспечения защиты информации
- выполнение функций ведомственного центра ГосСОПКА
- аудит безопасности и расследование инцидентов

Благодарю за внимание !

Вопросы ?

Столбов Андрей Павлович

stolbov_a_p@staff.sechenov.ru

ap100Lbov@mail.ru

ВЫСШАЯ
ШКОЛА
УПРАВЛЕНИЯ
ЗДРАВООХРАНЕНИЕМ
www.hsha.ru

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

[в условиях санкций]

- при необходимости двустороннего обмена данными МИ с внешними ИС следует использовать межсетевой экран и защищенный канал связи
- при необходимости односторонней передачи данных от МИ во внешние сети должны использоваться средства однонаправленной передачи данных ("инфодиоды"), исключающие передачу МИ управляющих команд извне
- если медорганизация не имеет возможности использовать защищенный канал передачи данных, МИ должно либо функционировать в составе изолированной сети, либо передача данных между различными компонентами МИ (например, между рабочей станцией оператора и АРМ врача) должна осуществляться с помощью переносных МНИ
- при отсутствия необходимости взаимодействия с внешними сетями МИ должны функционировать в составе локальной сети
- перед обновлением ПО необходимо создавать резервные копии – для возможности возврата к прежней версии ("отката назад")

Предложения в РГ Росздравнадзора от 13.04.2023:

- внесение изменений в приказ Минздрава РФ от 19.01.2017 № 11н в части расширения требований к содержанию техдокументации для цифровой медтехники – кибербезопасность, взаимодействие с внешними ИС, ИТ-сервисами, организация сопровождения ПО и др.
- разработка методики оценки киберзащищенности цифровых медицинских изделий

54% медорганизаций используют медтехнику с устаревшими ОС из-за чего произошли **32**% утечек данных и атак "шифровальщиков"

[Kaspersky Lab, 08.12.2021]

Постановления Правительства РФ

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 ИС персональных данных. – **№ 1119** от 01.11.2012

Правила категорирования и критерии значимости объектов КИИ РФ. – **№ 127** от 08.02.2018

Правила предоставления сведений, содержащихся в едином федеральном информационном регистре, содержащем сведения о населении РФ, перечень указанных сведений и срои их предоставления, и перечень обезличенных персональных данных (...) – **№ 1723** от 09.10.2021

Типовые положения: • о заместителе руководителя организации, ответственном за обеспечение информационной безопасности, • о структурном подразделении в организации, обеспечивающем информационную безопасность. – **№ 1272** от 15.07.2022

Требования к программному обеспечению (ПО), используемому на значимых объектах КИИ,
- Правила перехода на преимущественное использование российского ПО на объектах КИИ,
- Правила согласования закупок иностранного ПО (...) – **№ 1478** от 22.08.2022

Положение о единой биометрической системе (...) – **№ 883** от 31.05.2023

Перечень случаев, при которых аутентификация с использованием ИС, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, не допускается (...), и допускается (...) – **№ 815** от 25.05.2023

Порядок перехода субъектов КИИ РФ на преимущественное применение доверенных программно-аппаратных комплексов (ПАК) на принадлежащих им значимых объектах КИИ. – **№ 1912** от 14.11.2023 – запрет с 01.09.2024 использовать ПАК, не являющихся доверенными **!!**

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Правила категорирования и критерии значимости объектов КИИ РФ

– постановление Правительства РФ от 08.02.2018 № 127, в ред. от 20.12.2022 № 2360

Критерии присвоения категории значимости объектам КИИ (всего 14)

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

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

Nч – количество лиц, которые не смогут получить медицинскую помощь в полном объеме в течение времени восстановления Твос после компьютерного инцидента – расчет на основе статданных в ф. № 30 и среднего Твос. Если нет статистики за 5 лет, то Твос = 10 суток (см. Методрекомендации Минздрава РФ по категорированию объектов КИИ от 05.04.2021)

5. Отсутствие доступа к госуслуге: – см. № 2521-р от 15.11.2017, № 2113-р от 18.09.2019

а) допустимое время Тр (часов), в течение которого госуслуга может быть недоступна

III-я: 12 < Тр ≤ 24; **II-ая**: 6 < Тр ≤ 12; **I-ая**: Тр ≤ 6

б) время Тн с момента приема запроса на госуслугу, в течение которого она не может быть оказана – в % от времени её предоставления Тр из регламента

III-я: Тн ≤ 0.3 * Тр; **II-ая**: 0.3 * Тр < Тн ≤ 0.7 * Тр; **I-ая**: Тн > 0.7 * Тр

9. Возникновение ущерба бюджетам РФ – снижение отчислений в бюджет субъектом КИИ в % от прогноза годового дохода федерального бюджета – среднее за 3 года – Дфб

III-я: 3% < Дфб ≤ 70%; **II-ая**: 70% < Дфб ≤ 120%; **I-ая**: Дфб > 120%

Направление акта о категорировании ЗнОбКИИ в ФСТЭК, актуализация сведений – в течение 20 р/дней

Минздрав России – **мониторинг** предоставления сведений об ОбКИИ в ФСТЭК – пп. 19.2, 19.3

Разработка отраслевого перечня типовых объектов КИИ – п. 10(ж) (его согласование с ФСТЭК)

Приказы ФСБ России

Национальный координационный центр по компьютерным инцидентам (НКЦКИ). – № 366 от 24.07.2018 – **www.cert.gov.ru**

Перечень и порядок предоставления информации в ГосСОПКА. – № 367 от 24.07.2018

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

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. – № 368 от 24.07.2018

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

Порядок, технические условия установки и эксплуатации средств обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. – № 281 от 19.06.2019

Состав и содержание организационных и технических мер по обеспечению безопасности перс. данных при их обработке в ИС ПДн с использованием средств криптографической защиты информации. – № 378 от 10.07.2014

Требования о защите информации, содержащейся в ИС общего пользования. – приказ ФСБ и ФСТЭК России № 416/489 от 31.08.2010

Требования по обеспечению целостности, устойчивости функционирования и безопасности ИС общего пользования. – приказ Минкомсвязи РФ № 104 от 25.08.2009

ПНСТ 799-2022 Криптографическая защита информации. Термины и определения

Рекомендации по стандартизации:

- Р 1323565.1.043–2022 Контрольные примеры использования российских криптоалгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)
- Р 1323565.1.040–2022 Парольная защита ключевой информации
- Р 1323565.1.041–2022 Транспортный ключевой контейнер
- Р 1323565.1.048–2023 Использование российский криптоалгоритмов в протоколе обмена ключами в сети Интернет версии IKEv2

Приказы ФСТЭК России

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. – **№ 17** от 11.02.2013

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. – **№ 21** от 18.02.2013

Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования. – **№ 235** от 21.12.2017

Требования по обеспечению безопасности значимых объектов КИИ. – **№ 239** от 25.12.2017

Порядок согласования субъектом КИИ с ФСТЭК подключения значимого объекта КИИ к сети связи общего пользования. – № 75 от 28.05.2020

Требования по безопасности информации к средствам обеспечения безопасной дистанционной работы в ИС. – № 32 от 16.02.2021

Форма направления сведений о результатах присвоения объекту КИИ категории значимости. – № 236 от 22.12.2017

Порядок ведения реестра значимых объектов КИИ. – № 227 от 06.12.2017

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. – № 76 от 02.06.2020

Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. – № 77 от 29.04.2021

Методические документы ФСТЭК

Руководство по организации процесса управления уязвимостями в органе (организации). – 17.05.2023

Методика тестирования обновлений безопасности программных, программно-аппаратных средств. – 28.10.2022

Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств. – 28.10.2022

Рекомендации по безопасной настройке операционных систем Linux. – 25.12.2022

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении. – 25.12.2020

ГОСТ Р 59709-2022 Защита информации. Управление компьютерными инцидентами Термины и определения

ГОСТ Р 59710-2022 Защита информации. Управление компьютерными инцидентами Общие положения

ГОСТ Р 59711-2022 Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами

ГОСТ Р 59712-2022 Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты

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

ГОСТ Р 71206-2024 Защита информации. Разработка безопасного программного обеспечения. Безопасный компилятор языков С/С++. Общие требования

ГОСТ Р 71207-2024 Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования

* ТК 362 за 2022-2024 годы

Постановления Правительства России

Перечень случаев, при которых к операторам, осуществляющим трансграничную передачу персональных данных в целях выполнения возложенных международным договором РФ, законодательством РФ на государственные и муниципальные органы, функций, полномочий и обязанностей, не применяются требования частей 3–6, 8–11 ст. 12 закона "О персональных данных". – **№ 2526** от 29.12.2022

Правила принятия решения о запрещении или об ограничении трансграничной передачи персональных данных 'Роскомнадзором' и информирования операторов о принятом решении. – **№ 6** от 10.01.2023

Правила принятия решения 'Роскомнадзором' о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан. – **№ 24** от 16.01.2023

Приказы Роскомнадзора

Перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных. – № 128 от 05.08.2022

Требования к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения закона "О персональных данных". – **№ 178** от 27.10.2022

Требования к подтверждению уничтожения персональных данных. – № 179 от 28.10.2022

Формы уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных. – **№ 180** от 28.10.2022

Порядок и условия взаимодействия 'Роскомндзора' с операторами в рамках ведения реестра учета инцидентов в области персональных данных. – **№ 187** от 14.11.2022

Обезличивание медицинских данных

Федеральные законы

О персональных данных, **№ 152-ФЗ** от 27.07.2006
– ст. 3, ч. 3.1 ст. 4, ст. 5, пп. 9, 9.1 ч.1 ст. 6, ч. 2.1 ст. 10.

Об основах охраны здоровья граждан в РФ, **№ 323-ФЗ** от 21.11.2011
– п. 4 ч. 3 ст. 91.1, п. 9 ч. 4 ст. 91.1

Об экспериментальных правовых режимах в сфере цифровых инноваций в РФ, **№ 258-ФЗ** от 31.07.2020 – п. 13.1 ч. 5 ст. 10

Постановления Правительства РФ

Положение о Единой государственной информационной системе в сфере здравоохранения (ЕГИСЗ). **– № 140** от 09.02.2022

Положение о федеральной государственной информационной системе сведений санитарно-эпидемиологического характера.
– № 2178 от 02.12.2021 (в ред. постановления от 16.05.2023 № 756)

- ведение базы **обезличенных** данных со значениями биохимических исследований и общего анализа крови человека, полученных от организаций, осуществляющих клинико-диагностические лабораторные исследования

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования **дополнительной** информации определить принадлежность персональных данных конкретному субъекту персональных данных

[ст. 3 закона 152-ФЗ]

- Законопроект № 992331-7 от 21.07.2020
- Поручение Президента РФ от 08.09.2023 – принять закон до 15.12.2023

Обрабатываемые персональные данные подлежат **уничтожению** либо **обезличиванию** по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом [ч. 7 ст. 5 закона 152-ФЗ]

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 законами № 123-ФЗ и № 258-ФЗ [ч. 2.1 ст. 10 закона № 152-ФЗ]

– Кто оператор таких данных **?!** Лицензирование **?!**
– Кто вправе их использовать без согласия субъекта **?!**

ЕГИСЗ включает в себя сведения о лицах, которым оказывается медпомощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, осмотры и освидетельствования, **обезличенные** в порядке, установленным Минздравом РФ по согласованию с Роскомнадзором [п. 4 ч. 3 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 РФ **№ 341н** от 14.06.2018

Требования и методы по обезличиванию персональных данных.
– приказ Роскомнадзора **№ 996** от 05.09.2013

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

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

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

Приказ Росздравнадзора **№ 973** от 11.02.2022
– приложение № 1, п. 117 – проверка соблюдения порядка обезличивания

Федеральная интегрированная электронная медицинская карта (ФИЭМК)

- получение, проверка, обработка и хранение медицинских документов (СЭМД) и(или) сведений о состоянии здоровья гражданина, предоставленных с **согласия** гражданина (его законного представителя), или размещенных гражданином, в том числе посредством ЕПГУ, а также предоставление с его согласия доступа к ним медицинским работникам
- получение, проверка, обработка и хранение структурированных **обезличенных** сведений о лицах, которым оказывается медицинская помощь, в отношении которых проводятся медицинские экспертизы, осмотры и освидетельствования
- формирование баз данных **обезличенной** информации, позволяющих систематизировать информацию для изучения течения и исхода заболеваний, клинической и экономической эффективности методов профилактики, диагностики, лечения и реабилитации <...>
- хранение наборов **обезличенных** медицинских данных для их использования в целях создания алгоритмов и методов машинного обучения для формирования СППВР, создания и применения технологических решений на основе искусственного интеллекта (ИИ)
- поддержка: • разметки и подготовки наборов **обезличенных** медицинских данных, а также их верификации для решения конкретной задачи, в том числе с использованием методов машинного обучения; • разработки, хранения, функционирования и верификации технологических решений на основе ИИ, • доступ медорганизаций к этим решениям

[постановление № 140, пп. 13, 14]

Передача **обезличенных** данных о состоянии здоровья гражданина:

МИС МО -> ФИЭМК ЕГИСЗ

МИС МО -> ГИСЗ субъекта РФ

– **без** его **согласия** !!

– часть 2.1 ст. 10 закона № 152-ФЗ

Передача МО -> ФИЭМК
– в течение 1 рабочего дня со дня установления диагноза или со дня получения новых данных о пациенте
– постановления № 140, приложение № 1, п. 26

Порядок обезличивания
– см. приказ Минздрава России № 341н от 14.06.2018

Защита персональных данных в информационных системах здравоохранения: принципы и процедуры, применяемые в сфере охраны общественного здоровья. – Европейское региональное бюро ВОЗ. Копенгаген. 2021 г. – 30 стр.

Council for International Organizations of Medical Sciences (CIOMS) – cioms.ch

Международные этические руководящие принципы для исследований в области здоровья с участием людей. 4-ое издание. - Женева: CIOMS. – 2016 (рус. яз. 2018) – 25 руководящих принципов: № 12 – Сбор, хранение и использование данных в исследованиях; № 22 – Использование данных, полученных из онлайн-среды и с помощью цифровых средств, в научных исследованиях

European Commission – commission.europa.eu

General Data Protection Regulation (**GDPR**), Regulation (EU) 2016/679, 04.05.2016

Data Governance Act (**DGA**), Regulation (EU) 2022/868, 30.05.2022 \ с 24.09.2023

European Union Agency for Cybersecurity (ENISA) – enisa.europa.eu

Cloud Security for Healthcare Services. – 18.01.2021

Data Pseudonymisation: Advanced Techniques and Use Cases. – 28.01.2021

Deploying Pseudonymisation Techniques. – 24.03.2022

Engineering Personal data sharing. Emerging Use Cases and Technologies. – 27.01.2023

Cybersecurity and privacy in AI - Medical imaging diagnosis. – 07.06.2023

Столбов А.П. Обезличивание персональных данных в здравоохранении. Врач и информационные технологии, 2017, № 3, сс. 76-91.

NHS: база данных выписных эпикризов – доступ через платформу Spine