ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕДИЦИНЕ

ИТМ 2023

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

# Кибербезопасность медицинской деятельности: обзор новых нормативных актов


Сеченовский Университет

ИНСТИТУТ ЛИДЕРСТВА и УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ
www.hsha.ru

**Столбов Андрей Павлович**


**13 октября 2023 г.**

## Указы Президента РФ

О создании, развитии и эксплуатации государственных информационных систем с использованием единой цифровой платформы РФ "ГосТех". – **№ 231** от 31.03.2023

ФГИС – с 01.04.2023, рег. ГИС – с 01.01.2024

## Проекты указов

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

О внесении изменений в Указ от 01.05.2022 № 250 – 20.06.2023

## Постановления Правительства РФ

Положение о единой цифровой платформе РФ "ГосТех". – **№ 2338** от 16.12.2022

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 (в ред. от 16.12.2022 № 2338)

## Распоряжения Правительства РФ

Концепция создания и функционирования единой цифровой платформы РФ "ГосТех". – **№ 3102-р** от 21.10.2022

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

Концепция информационной безопасности детей в Российской Федерации (..) – **№ 1105-р** от 28.04.2023

## 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

## 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)

**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 среднего годового дохода федерального бюджета 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 с привлечением подведомственных организаций (по согласованию с ФСТЭК) для оценки актуальности и достоверности сведений – пп. 19.2, 19.3

Разработка отраслевого перечня типовых объектов КИИ **!?**

– п. 10(ж) (его согласование с ФСТЭК)

## Требования по обеспечению безопасности значимых объектов КИИ.

– приказ ФСТЭК от 25.12.2017 **№ 239** (в ред. от 20.02.2020 № 35) – с 01.01.2023

- Требования к классам защиты и уровням доверия к сертифицированным СЗИ – в зависимости от категории значимости объектов КИИ (п. 29)

  – см. приказ ФСТЭК № 76 от 02.06.2020

- Требования по безопасной разработке (модернизации), испытаниям и поддержке безопасности **прикладного** ПО значимого объекта КИИ (п. 29.3):
  - наличие руководства по безопасной разработке ПО
  - проведение анализа угроз безопасности информации ПО
  - выявление уязвимостей (статический и динамический анализ кода, фаззинг-тестирование)
  - наличие процедур отслеживания и исправления ошибок, уязвимостей и др.
  - определение способов и сроков доведения до пользователей информации об уязвимостях ПО, о компенсирующих мерах по защите информации или ограничениях по применению ПО, способов получения пользователями обновлений ПО, проверки их целостности и подлинности

**ГОСТ Р**
51583, 51583, 56545, 56546, 59494,
**ГОСТ Р ИСО/МЭК**
27034-2, 27034-3, 27034-5, 27034-6, 27034-7, 27036-4, 21827

## Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования.

– приказ ФСТЭК от 21.12.2017 **№ 235** (в ред. от 20.04.2023 № 69)

- Возможность привлечения специалистов со средним профобразованием по ИБ
- Сокращены сроки переподготовки специалистов по ИБ с 5 до 3 лет
- Обязательные компенсирующие меры при невозможности техподдержки СЗИ со стороны производителя

## Методические документы ФСТЭК

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

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

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

---

**ГОСТ Р Защита информации. Управление компьютерными инцидентами**

ГОСТ Р 59709-2022 – Термины и определения

ГОСТ Р 59710-2022 – Общие положения

ГОСТ Р 59711-2022 – Организация деятельности по управлению компьютерными инцидентами

ГОСТ Р 59712-2022 – Руководство по реагированию на компьютерные инциденты

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

## Инфосообщение ФСТЭК

О порядке представления субъектами КИИ сведений о результатах присвоения объектам КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.
– № 240/82/818 от 28.04.2023

## Приказы ФСТЭК

Требований по безопасности информации к средствам виртуализации.
– № 187 от 27.10.2022

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

## Приказы ФСБ России

Об определении переходного периода, предусмотренного пп. "б" п. 5 Указа Президента РФ от 01.05.2022 № 250.
– **№ 543** от 01.11.2022 = 3 года – ГосСОПКА по договору с НКЦКИ

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, со ЗнОбКИИ – 3 ч., с иным ОбКИИ – 24 ч.
- Не субъект КИИ -> Роскомнадзор -> НКЦКИ – 24 ч., рассл. – 72 ч.

Порядок осуществления мониторинга защищенности информационных ресурсов, принадлежащих ФОИВ, высшим ИОГВ субъектов РФ, государственным фондам, госкомпаниям, иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим АО и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами КИИ либо используемых ими.
– **№ 213** от 11.05.2023

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

---

ПНСТ 799-2022 Криптографическая защита информации. Термины и определения.

Рекомендации по стандартизации:

- Р 1323565.1.043–2022 Криптографическая защита информации. Контрольные примеры использования российских криптоалгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)
- Р 1323565.1.040–2022 Криптографическая защита информации. Парольная защита ключевой информации.
- Р 1323565.1.041–2022 Криптографическая защита информации. Транспортный ключевой контейнер.

# 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 50720 уязвимостей

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

---

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 план импортозамещения ИТ в здравоохранении **?!**

---

Методические рекомендации по переходу на использование российского ПО, в том числе на значимых объектах КИИ, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского ПО.
– приказ Минцифры России № 21 от 18.01.2023

# 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
  – **с 01.03.2023** – части 8, 9, 10 ст. 10 закона № 149-ФЗ
  (закон № 584-ФЗ от 29.12.2022)

**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
- проведении вступительных испытаний, промежуточной и итоговой аттестации с использованием дистанционных образовательных технологий

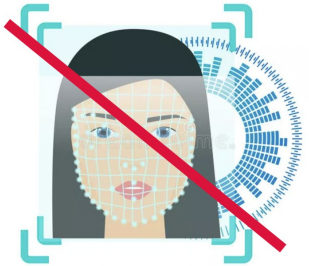
Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных <..>

– федеральный закон **№ 572-ФЗ** от 29.12.2022

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

Перечень случаев, при которых аутентификация с использованием ИС организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, не допускается <..> и при которых допускается <..>

– постановление Правительства России **№ 815** от 25.05.2023



## Федеральный закон № 406-ФЗ от 31.07.2023

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

- авторизация пользователей в российских ИС при доступе через Интернет – с помощью: • номера мобильного телефона, • ЕСИА, • ЕБС, • иных российских ИС, соответствующих требованиям защиты информации, установленным ст. 16 закона № 149-ФЗ – с 01.12.2023
- уведомление Роскомнадзора о предоставлении вычислительной мощности для размещения информации в ИС, подключенной к сети Интернет – 01.12.2023
- предоставление хостинга без включения в реестр Роскомнадзора запрещено – с 01.02.2024
- порядок ведения реестра, включения и исключения из реестра устанавливаются Правительством РФ
- операторы ГИС, ИС государственных и муниципальных предприятий и учреждений должны использовать вычислительные мощности провайдера хостинга, включенного в реестр, и не вправе использовать мощности, принадлежащие иностранным лицам – с 01.09.2024

  – ч.10 ст.8, ст.10.2-1, ст.10.4, ч.2.1-1, -2, ч.2.4 ст.13, п.1 ч.5 ст.15.1 № 149-ФЗ

ЕСИА

# Благодарю за внимание !

# Вопросы ?

**Столбов Андрей Павлович**

**stolbov_a_p@staff.sechenov.ru**

**ap100Lbov@mail.ru**

Сеченовский Университет
ИНСТИТУТ ЛИДЕРСТВА и УПРАВЛЕНИЯ ЗДРАВООХРАНЕНИЕМ
www.hsha.ru