Министерство здравоохранения Российской Федерации
«НАЦИОНАЛЬНЫЙ МЕДИЦИНСКИЙ ИССЛЕДОВАТЕЛЬСКИЙ
ЦЕНТР ТЕРАПИИ И ПРОФИЛАКТИЧЕСКОЙ МЕДИЦИНЫ»

Кибербезопасность медицинской деятельности. Организация обработки и защиты персональных данных

Орлов Сергей Александрович

старший научный сотрудник отдела научно-стратегического развития первичной медико-санитарной помощи, к.м.н.

Конфликт интересов отсутствует

- Отказ всей цифровой техники в Центре нейрохирургии во время операции в результате хакерской атаки [*ТАСС, 06.07 2018*]
- Нарушение работоспособности ЛИС областного онкодиспансера из-за хакерской атаки [*Медвестник, 01.09.2020*]
- Утечка персональных данных более 30 млн. клиентов медицинской компании "Гемотест" [*ТАСС, 04.05.2022*]
- 2022 год – утечка персональных данных 85% взрослого населения России
- ("Почта России", "Гемотест", "Яндекс.Еда", "Спортмастер" и др.) [Роскомнадзор, 18.01 2023]
- 2022 год – утечка персональных данных в 20% медицинских организаций РФ [СёрчИнформ, 16.02.2023]

Взлом ЕПГУ - февраль 2015 ... октябрь 2022

Удаленная работа, телемедицина "врач – пациент", m-Health
-> высокие риски нарушения ИБ

Глобализация кибератак, низкая киберзащищенность цифровой медтехники

в **54**% медорганизаций РФ используется медтехника с устаревшими ОС из-за чего произошли **32**% утечек данных, DDoS-атак и атак "шифровальщиков" [Kaspersky Lab, 08.12.2021]

Рост затрат на ИБ

82% – преднамеренные утечки (2022)
(в 2021 было 58.3%)

79% инцидентов – из-за низкой организации, незнания (57%) и халатности (22%)
[Kaspersky Lab, 19.04.2023]

Федеральные законы

Конституция Российской Федерации, 12.12.1993
– ст. 23, ст. 24

О персональных данных, **№ 152-ФЗ** от 27.07.2006

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

Гражданский кодекс РФ, № 51-ФЗ от 30.11.1994
– статьи 152.х

Трудовой кодекс РФ, № 197-ФЗ от 30.12.2001
– статьи 86-90

О коммерческой тайне, № 98-ФЗ от 29.07.2004

Об организации предоставления государственных и муниципальных услуг, № 210-ФЗ от 27.07.2010

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

О едином федеральном информационном регистре, содержащем сведения о населении РФ, **№ 168-ФЗ** от 08.06.2020

Об осуществлении идентификации и аутентификации физических лиц с использованием биометрических персональных данных (..), **№ 572-ФЗ** от 29.12.2022

О защите прав потребителей, № 2300-I от 07.02.1992

Об образовании в Российской Федерации, № 273-ФЗ от 29.12.2012

О физической культуре и спорте в Российской Федерации, № 329-ФЗ от 04.12.2007

Об обязательном медицинском страховании в Российской Федерации, № 326-ФЗ от 29.11.2010

Об основах охраны здоровья граждан в Российской Федерации, **№ 323-ФЗ** от 21.11.2011

О психиатрической помощи и гарантиях прав граждан при её оказании, № 3185-I от 02.07.1992

О донорстве крови и ее компонентов, № 125-ФЗ от 20.07.2012

О трансплантации органов и(или) тканей человека, № 4180-I от 22.12.1992

О предупреждении распространения в РФ заболевания, вызываемого ВИЧ, № 38-ФЗ от 30.03.1995

О предупреждении распространения туберкулеза в Российской Федерации, № 77-ФЗ от 18.06.2001

<...>

Указы Президента Российской Федерации

Об утверждении перечня сведений конфиденциального характера, № 188 от 06.03.1997

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

Доктрина информационной безопасности РФ, № 546 от 05.12.2016

Стратегия развития информационного общества в РФ на 2017-2030 годы, № 203 от 09.05.2017

Основы государственной политики РФ в области международной информационной безопасности, № 213 от 12.04.2021

О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации, № 166 от 30.03.2022

О дополнительных мерах по обеспечению информационной безопасности Российской Федерации, **№ 250** от 01.05.2022 !!

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О дополнительных мерах по обеспечению информационной безопасности Российской Федерации

В целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации п о с т а н о в л я ю:

1. Руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (далее - органы (организации):

Президент
Российской Федерации В.Путин

Москва, Кремль
1 мая 2022 года
№ 250

Постановления Правительства РФ

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

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

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 <...>, **№ 815** от 25.05.2023

Концепция информационной безопасности в сфере здравоохранения

– утверждена Правительственной комиссией по цифровому развитию <...>, протокол № 7 от 10.03.2022, опубликована 22.06.2022, – 85 с. !!

Отраслевой **Центр информационной безопасности** и импортозамещения ПО !!

– на базе ЦНИИОИЗ

Приказы и методические документы Минздрава России

- Порядок обезличивания сведений о лицах, которым оказывается медицинская помощь, в отношении которых проводятся медицинские экспертизы, осмотры и освидетельствования. – приказ **№ 341н** от 14.06.2018
- Требования к государственным ИС в сфере здравоохранения субъектов РФ, МИС медицинских организаций (МИС МО), ИС фармацевтических организаций. – приказ **№ 911н** от 24.12.2018
- 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
- Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения. – 05.04.2021, – 175 с.
- Методические рекомендации медицинским организациям по организации криптографической защиты каналов при взаимодействии в рамках ЕГИСЗ. – 31.08.2023, – 15 с.

Уполномоченные органы в области защиты информации

- Федеральная служба по техническому и экспортному контролю
  - **ФСТЭК – www.fstec.ru**
  - техническая защита информации, обеспечение безопасности объектов КИИ
- Федеральная служба безопасности
  - **ФСБ – www.fsb.ru**
  - обращение средств криптографии, обеспечение работы ГосСОПКА

- **Национальный координационный центр по компьютерным инцидентам**
  - **НКЦКИ – www.cert.gov.ru**

  incident@cert.gov.ru - для сообщений о компьютерных инцидентах

Уполномоченный орган по защите прав субъектов персональных данных

- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
  - **Роскомнадзор – www.rkn.gov.ru**
  - государственный контроль и надзор за соответствием обработки персональных данных требованиям законодательства

- **Центр правовой помощи гражданам в цифровой среде**
  - **www.4people.grfc.ru**

Обязанность мед.организации сообщить в НКЦКИ и Роскомнадзор об киберинциденте и утечке персональных данных !!

Термины и определения (1)

Информация - сведения (сообщения, данные) независимо от формы их представления

Доступ к информации - возможность получения и использования информации

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора **право разрешать или ограничивать** доступ к информации, определяемой по каким-либо признакам

Информация ограниченного доступа - доступ к которой ограничен в соответствии с **федеральными** законами

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование **не распространять** и **не передавать** её третьим лицам **без согласия** её **обладателя**

Распространение информации - действия, направленные на получение информации **неопределенным** кругом лиц - публикация в СМИ, в сети Интернет, "на заборе" *etc*

Предоставление (передача) информации - действия, направленные на получение информации **определенным** кругом лиц или её передачу определенному кругу лиц

Раскрытие информации - обеспечение доступа **неограниченного** круга лиц к **определенной** информации в соответствии с процедурой, гарантирующей нахождение и получение указанной информации, **независимо от цели** ее получения

[закон № 149-ФЗ]

! Разглашение информации - несанкционированное **доведение** защищаемой информации **до лиц, не имеющих права доступа** к этой информации

[ГОСТ Р 53114-2008 Защита информации. Термины и определения]

Термины и определения (2)

Информационная безопасность (ИБ) - защищенность от случайного или преднамеренного вредоносного воздействия на информационные и технологические системы

Характеристики **безопасности информации**:

- **конфиденциальность** - защита от несанкционированного доступа (НСД) к защищаемой информации - получение доступа только авторизованным пользователям (кому разрешено)
- **целостность** - защита от несанкционированого удаления или изменения данных (информации)
- **доступность** - возможность пользователя беспрепятственно реализовать установленные ему права доступа к определенной информации (чтение, запись, изменение, удаление) в ИС

Кибербезопасность - информационная безопасность при работе в сети, в том числе в сети Интернет

Угроза информационной безопасности - совокупность условий и факторов, создающих опасность нарушения информационной безопасности

Нарушитель - лицо, случайно или преднамеренно осуществляющее действия, приводящие к нарушению безопасности информации

Утечка информации - неконтролируемое нарушение конфиденциальности (распространение, предоставление) защищаемой информации

Защита информации - комплекс **правовых**, **организационных** и **технических** мер, направленных на:

- предотвращение потери, искажения и несанкционированного доступа к ресурсам ИС
- предотвращение неправомерного блокирования доступа пользователей к информации, обрабатываемой в ИС
- ликвидацию последствий нарушения фунционирования ИС после сбоев и компьютерных атак (востановление)

[ГОСТ Р 50922, ГОСТ Р 56546]

Модель угроз информационной безопасности

- перечень актуальных угроз ИБ с оценкой возможных последствий их реализации:
  - каналы утечки,
  - типы нарушителей,
  - оценка рисков, ущерба, вреда и др.
- утверждает руководитель медорганизации !!

Возможные **каналы утечки и воздействия** на ИС

- линии связи, сети передачи данных, Интернет
- беспроводные каналы Wi-Fi, BlueTooth -> перехват
- ноутбуки, смартфоны, планшеты -> утеря, кража
- внешние носители данных -> утеря, кража
- аудио- и визуальный -> прослушивание, просмотр – мобильный телефон – "полицейский" режим !!
- человек, инсайдер – основной источник утечки !!

Объекты защиты

- компьютеры, серверы и программное обеспечение
- персональные данные, медицинские документы (ЭМК)
- цифровая медицинская техника
- каналы передачи данных – телекоммуникационная техника
- некоторые сведения о системе защиты информации

Принципы защиты информации

- Принцип **"враждебного окружения"**
  - все внутренние пользователи
  - это потенциальные нарушители,
  - все внешние - хакеры
- Принцип **"нулевого доверия"**
  -тотальная многофакторная аутентификация, авторизация доступа, **учетность** и **неотказуемость**
- Разумная достаточность, **комплексность** и **равнопрочность** системы защиты информации

Термины и определения (3)

Объекты КИИ - информационные системы (ИС), телекоммуникационные сети (ТКС) и автоматизированные системы управления технологическими процессами субъектов КИИ

Субъекты КИИ - госорганы, российские юрлица, индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат **объекты КИИ**, функционирующие в сфере **здравоохранения**, науки, транспорта, энергетики, финансов *etc*

Объекты КИИ в здравоохранении - МИС, цифровая медицинская техника (АСУ) и каналы (сети) передачи данных (ТКС)

Медицинская организация – субъект КИИ !! ->

- создать комиссию по категорированию ОбКИИ
- выявить объекты КИИ и определить их категории значимости - см. постановление Правительства РФ от 08.02.2018 № 127
- направить сведения о значимых ОбКИИ в ФСТЭК - см. приказ ФСТЭК № 236 от 22.12.2017

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

Нарушение ИБ или функционирования **МИС** и(или) цифровой **медицинской техники** ->

- утечка конфиденциальной информации
- потеря или искажение медицинских данных и(или) медицинских документов
- отказ или несанкционированное изменение режима работы медтехники

-> угроза жизни и здоровью !!

При выявлении компьютерного инцидента – незамедлительно сообщить в ФСБ – в НКЦКИ !! [ст. 9 закона № 187-ФЗ]

Перечень типовых объектов КИИ в здравоохранении

– отраслевой Центр информационной безопасности в ЦНИИОИЗ (проект)

Правила категорирования и критерии значимости объектов КИИ РФ

- постановление Правительства РФ от 08.02.2018 № 127

Критерии присвоения категории значимости объектам КИИ (всего 14) → в зависимости от вреда, ущерба в результате киберинцидента

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 **?!**

Направление акта о категорировании ОбКИИ 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

Персональные данные (ПДн)

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность *[Указ Президента РФ № 188 от 06.03.1997]*
- любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу - субъекту персональных данных *[закон № 152-ФЗ]*

Профессиональная тайна - информация, полученная физическими лицами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности:

- подлежит защите, если на эти лица федеральными законами возложены обязанности по соблюдению её конфиденциальности
- может быть предоставлена третьим лицам в соответствии с федеральными законами и(или) по решению суда.

Обязанность хранить врачебную тайну пожизненно !!

[ст. 9 закон № 149-ФЗ]

Персональные данные в медицинской организации

- Пациентов (о состоянии здоровья – спец. категория)
- Представителей пациентов

  - законные (родители, усыновители, опекуны)

  - иные лица, указанные пациентом, которым могут быть переданы сведения о его здоровье

} В медицинских документах

- Работников организации и членов их семьи
- Лиц, работающих по договору подряда
- Соискателей вакансий

} В отделе кадров, в бухгалтерии

Оператор персональных данных

– юридическое или физическое лицо, которое:
  - самостоятельно или совместно с другими лицами организует и(или) осуществляет обработку персональных данных и
  - определяет цели их обработки, состав данных и выполняемые с ними действия

Обработке подлежат только персональные данные, которые отвечают заранее заявленным **целям** их обработки (ст. 5)

Цели и состав персональных данных, обрабатываемых при осуществлении определенных видов деятельности, установлены федеральными законами
-> **персонифицированный учет**
  - статьи 93, 94 закона № 323-ФЗ
  - ст. 44 закона № 326-ФЗ

- "неизбыточность" состава данных **!!** (ст. 5)

Обработка персональный данных третьим лицом - **только с согласия** субъекта, если иное не предусмотрено законом (ст.6)

Примеры: использование "облачной" МИС, хостинг сайта на сервере провайдера, ТМ-система *etc*

Ответственность перед субъектом персональных данных за их безопасность **несет оператор !!** Обработчик несет ответственность перед оператором.

Право субъекта на **возмещение убытков** и **компенсацию морального вреда** в случае нарушения порядка обработки его персональных данных (ст.17)

[закон № 152-ФЗ]

- -

Средний размер компенсации – 84 тыс. руб

[журнал "Закон", март 2020]

"Пациентский экстремизм" + Судебное (юридическое) "инвестирование" **!?**

Оператор (медорганизация) обязан:

- определить перечень лиц, допущенных к обработке различных категорий конфиденциальной информации, персональных данных -> приказ
- назначить ответственного з**а организацию обработки** персональных данных (ст. 22.1)
  - доводить до сведения работников требования законов и иных нормативных документов
  - осуществлять внутренний контроль (аудит) – не реже 1 раза в 3 года
  - организовывать прием и обработку обращений субъектов персданных – ответ не позднее 10 дней
  - проводить **оценку вреда** субъекту при нарушении требований закона № 152-ФЗ
    - см. приказ Роскомнадзора № 178 от 27.10.2022
    - (вне)штатная должность: квалификация,трудозатраты **?!**
- опубликовать на своем сайте документы, определяющие политику обработки персональных данных и реализации требований по их защите (ст. 18.1)
- назначить ответственного **за защиту** персональных данных и объектов КИИ
  - разделение функций и ответственности:
    - за ИБ и • за фукционирование ИС **!!**
- организовать получение и хранение согласий на обработку персональных данных при необходимости получить согласие субъекта на распространение его персональных данных, разрешенных для распространения
  -это "отдельное" согласие (ст. 10.1) - см. приказ Роскомнадзора № 18 от 24.02.2021
- предупредить субъекта об аутсорсинге обработки персданных и получить его согласие на это + опубликовать на сайте сведения об аутсорсере (ст. 6 закона № 152-ФЗ)
- создать систему защиты информации - надо издать около **30** организационно-распорядительных документов **!!** (ст. 19 закона № 152-ФЗ, ст. 9 закона № 187-ФЗ)

Правомочность обработки персональных данных (ст. 5,6)

- с согласия субъекта (или его представителя), либо
- без согласия – на основании федерального закона

Согласие субъекта на обработку его ПД должно быть **конкретным, информированным и сознательным** (ст.9)

- цель обработки + кому и в каких случаях передаются данные
- состав обрабатываемых персонифицированных данных
- перечень выполняемых действий (операций) с данными

Согласие на обработку персональных данных (ОПДн):

- в письменной форме, в т.ч. в виде электронного документа (ст. 9 152-ФЗ – форма письменного согласия; возможно – по доверенности, оформленной в простой письменной форме (ст. 185 ГК РФ)
- в иной форме – в виде действия, совершаемого субъектом после ознакомления с условиями и порядком обработки персональных данных (через web-сайт) – **договор присоединения** (ст. 428 ГК РФ) – пометка о согласии в электронном «бланке» / форме

Согласие на ОПДн – для одного / каждого отдельного оператора !!
[закон № 152-ФЗ]

Право субъекта персданных на получение от оператора информации:

- о подтверждении факта обработки его персданных оператором
- о **правовых основаниях, целях**, способах и сроках их обработки, сроках хранения
  – пп. 2.3, 3, 4, 8 ч. 2, ч. 2.1 ст. 10 закона № 152-ФЗ, ст. 93, 94 закона № 323-ФЗ, ст. 44 закона № 326-ФЗ
- о лицах, имеющих доступ к его персданным или которым они могут быть предоставлены на основании договора с оператором или федерального закона *) - за исключением работников оператора
  – Росздравнадзор, Роспотребнадзор, фонды ОМС, СМО, другие МО, СФР *etc*

- о лицах, осуществляющих обработку его персданных по поручению оператора (аутсорсерах) (ст. 6) -> опубликовать на сайте оператора **!!**
  - при хостинге сайта на сервере провайдера, при использовании "облачной" МИС *etc*
- о трансграничной передаче его персональных данных

о своих персональных данных и источниках их получения

*) Оператор вправе отказать субъекту в получении этих сведений, если обработка осуществляется в целях обеспечения охраны правопорядка, государственной или транспортной безопасности

[ст. 14, 18, 20 закона № 152-ФЗ]

Специальные категории персональных данных

(ст. 10 закона № 152-ФЗ)

- о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, **состоянии здоровья**, интимной жизни - их обработка допускается только если:

- субъект дал согласие на их обработку в письменной форме (п.1)
- субъект сделал их общедоступными (п.2)
- их обработка осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым и пенсионным законодательством (п.2.3)
- их обработка необходима для защиты **жизни и здоровья** или иных жизненно важных интересов субъекта либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта невозможно (п.3)
- их обработка осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что их обработка осуществляется лицом, занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну (п.4)

- их обработка осуществляется в соответствии с законодательством об обязательных видах страхования, страховым законодательством (п.8)

– сведения о группе крови, инвалидности **?!**

Биометрические персональные данные (ст. 11)

- сведения, которые:

- **позволяют** установить личность человека
- **используются** оператором **для установления** его личности - для аутентификации

Биометрическая аутентификация
- только с **письменного согласия** человека **!!**

Rx-снимки, геномные данные (ДНК) в медицинской организации **не относятся** к биометрическим данным - **согласие** на их обработку **не нужно !!**

Публикация фото (видео) гражданина в Интернет, на стенде, в рекламных материалах *etc*
- **только** с его **письменного согласия !!**
- ст. **152.1** ГК РФ Защита изображения гражданина

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне ИС персональных данных.
– постановление Правительства РФ № 512 от 06.07.2008

Запрет биометрической **аутентификации** при:
- оказании медицинской помощи
- получении информированного добровольного согласия на медицинское вмешательство или отказ от него
- получении медицинских документов (их копий)
- проведении дистанционных медосмотров работников и контроля за их состоянием
- отпуске лекарственного препарата по рецепту
- предоставлении государственных и муниципальных услуг
- предоставлении доступа к государственным ИС
  – с 01.06.2023 !! – постановление № 815

Единая система биометрической идентификации
- право **отказа (запрета)** от биометрической идентификации и аутентификации
- интеграция с ЕСИА

[закон № 572-ФЗ]

Видеонаблюдение (аудиовидеозапись) на рабочем месте **медработника** разрешается **без согласия** пациента !!

Приказ об организации видеонаблюдения, допуске работников к видеозаписям, хранении и уничтожении записей (места, сроки), порядке получения пациентом копии видеозапии

Цель - обеспечение личной безопасности, контроль качества работы, обеспечение сохранности имущества – п.1 ч.1 ст. 86 ТК РФ

- Предупреждение о ведении видеонаблюдения на рабочих местах в трудовом договоре + право на просмотр видеозаписей "о себе"
- Объявления на видных местах о ведении видеонаблюдения на приеме врача и при выполнении процедур !!
- Видеонаблюдение не во время приема и в комнатах отдыха запрещено !! (неприкосновенность частной жизни работника)
- Получение пациентом копии видеозаписи - с учетом требований ст. 152.1 ГК РФ (охрана изображения гражданина) - передача третьим лицам - только **с письменного согласия** медработника !!
- При использовании видеозаписей для обучения, в научных или иных целях - получить **письменное согласие** медработников и пациентов либо обезличить запись (сокрытие лица, удаление или изменение тембра речи, удаление речи, содержащей Ф.И.О.

Вправе ли пациент запретить ведение видеозаписи на приеме врача в медорганизации **?!** На дому **?!** При анонимном оказании медпомощи **?!**

Видеозапись приема по просьбе пациента на его устройство

(в помещении МО, в автомобиле СМП, при посещении на дому)

- Медработник **не может запретить** пациенту делать аудиовидеозапись **!!**
- Видеосъемка не должна мешать медработнику **!!**
- Запись в медкарте (?) о видеозаписи по просьбе пациента на его устройство **?!**
- Предупредить пациента о запрете распространения и(или) передаче видеозаписи третьим лицам - ст. 152.1 ГК РФ
- Предупредить пациента об ответственности за нарушение этого требования - ст. 13.11 КоАП РФ (штраф от 2 до 6 тыс. руб) и о возможном иске о компенсации морального вреда - ст. 150 ГК РФ

Объявление о **запрете** фото- и видеосъемки в помещениях медицинской организации **без разрешения** администрации и ответственности за нарушение по ст. 13.11 КоАП **!!**

Перед видеосъемкой представителями СМИ посетители и медперсонал должны быть об этом **предупреждены** -> только с их **согласия** **!!**

Решение Верховного суда РФ (декабрь 2019)
– "скрытные" аудио- и видео- записи могут приниматься судами к рассмотрению

Порядок организации и деятельности федеральных учреждений МСЭ –приказ Минтруда РФ № 979н от 30.12.2020 – п.19

- аудиовидео-фиксация при проведении МСЭ
- срок хранения аудио-видеоматериалов (АВМ) – 90 дней
- ознакомление с АВМ и получение их копии гражданином – в срок до 30 дней
- право гражданина проводить видеозапись на свое устройство

Статья 152.1. Охрана изображения гражданина (ГК РФ)

Обнародование и дальнейшее использование изображения гражданина (фотографии, видеозаписи, произведения искусства, в которых он изображен) допускаются **только с согласия** этого гражданина.

После смерти гражданина его изображение может использоваться только с согласия детей и пережившего супруга, а при их отсутствии - с согласия родителей.

Согласие **не требуется**, если:

1) использование изображения осуществляется в государственных, общественных или иных публичных интересах
2) изображение гражданина получено при съемке, которая проводится в местах свободного посещения или на публичных мероприятиях (собраниях, конференциях, представлениях, спортивных соревнованиях и т.д.), за исключением случаев, когда такое изображение является основным объектом использования
3) гражданин позировал за плату.

-> Оформить **согласие** работника, пациента **на публикацию** его фото (видео) на сайте, на стенде, в рекламных материалах, в сети Интернет **!!**

Трансграничная передача персональных данных (ст. 12)

- на территорию иностранного государства, органу власти иностранного государства, иностранному физическому или юридическому лицу
- **с согласия** гражданина РФ или на основании договора с ним (ч. 1.1 ст. 1)
  – ТМ-консультации, передача документов для лечения за рубежом

Оператор **до начала** осуществления деятельности по трансграничной передаче персданных **обязан уведомить** об этом Роскомнадзор. Уведомление должно содержать:

- Ф.И.О. и "контакты" ответственного за организацию обработки персданных
- правовое основание и цель передачи персданных и их дальнейшей обработки
- категории и перечень передаваемых персональных данных
- категории субъектов персональных данных, чьи данные передаются
- перечень иностранных государств, куда планируется передача персданных
- дату проведения оператором оценки соблюдения органами власти иностранных государств и иностранными операторами конфиденциальности и обеспечения безопасности персданных – оператор обязан предварительно получить от них соответствующие сведения и документы

– формы уведомлений – см. **pd.rkn.gov.ru/cross-border-transmission/**

См. постановления Правительства РФ :

• № 2526 от 29.12.2022, • № 6 от 10.01.2023, • № 24 от 16.01.2023

+ приказ Роскомнадзора № 128 от 05.08.2022,

Согласие на обработку персональных данных – закон № 152-ФЗ

Согласие субъекта на обработку его персональных данных **не требуется:**

- при оказании ему медицинской помощи
- для выполнения договора в его интересах

Пациент **не может запретить** обработку его персональных данных в медорганизации **!!**

– пп. 3, 4 ч.2 ст. 10, п. 5 ч.1 ст. 6

Согласие на обработку персональных данных

- в письменной форме, и в виде ЭД (ст. 9)
- в форме договора присоединения (ст. 428 ГК РФ)

Может быть подписано **по доверенности**, в том числе в простой письменной форме (ст. 185 ГК РФ)

Должно содержать: цель обработки, состав сведений, перечень выполняемых действий, кому, когда и какие данные передаются + **риски**

Согласие необходимо:

- при передаче персональных данных по открытым каналам связи – по e-Mail, на сайт ...
- при обработке персональных данных аутсорсером (ст. 6)
- при трансграничной передаче персональных данных (ст. 12)
- при распространении оператором персональных данных, разрешенных субъектом для распространения (ст. 10.1)
  – приказ Роскомнадзора № 18 от 24.02.2021
- при передаче персданных третьему лицу и это не предусмотрено договором или законом
- при хранении сканов паспортов, военных билетов и других документов "личного хранения" пациентов и работников
- при использовании биометрических данных для установления личности (ст. 11)

Законодательные новеллы в отношении Оператора (медорганизации)

- при обнаружении утечки персданных - уведомить Роскомнадзор: - в течение 24 часов – о факте и о возможных причинах; - в течение 72 часов – о результатах внутреннего расследования – см. приказ Роскомнадзора No 187 от 14.11.2022
- информировать ФСБ об инцидентах, приведших к утечке персданных и взаимодействовать с ГосСОПКА – см. приказ ФСБ № 77 от 13.02.2023
- обязательно уведомить Роскомнадзор о намерении осуществлять обработку персональных данных (и её прекращении)
- уведомлять Роскомнадзор об изменениях в организации защиты персданных – до 15-го числа следующего месяца – см. приказ Роскомнадзора № 180 от 28.10.2022
- уведомлять Роскомнадзор о трансграничной передаче персональных данных – см. **pd.rkn.gov.ru/cross-border-transmission/**

Роскомнадзор ведет реестр учета инцидентов в области персональных данных и передает эти данные в ФСБ.

Приказы Роскомнадзора

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

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

Приказ ФСБ России

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

Работодатель имеет **право контролировать**:

- содержание данных, состав программного обеспечения на служебном компьютере работника
- входящий и исходящий трафик – переписку, посещение сайтов *etc*, а также
- трафик при выходе в Интернет с личного устройства через служебную сеть (WiFi),

– если это предусмотрено трудовым договором.

Порядок контроля должен быть описан в трудовом договоре.

Работники и их представители должны быть ознакомлены под роспись с документами, устанавливающими порядок обработки их персональных данных, а также об их правах и обязанностях в этой области.

– ст. 86 ТК РФ

Должностные обязанности (инструкции) должны содержать:

- перечень сведений конфиденциального характера (персональные данные, врачебная тайна, коммерческая тайна и т.п.), доступ к которым имеет работник
- перечень мер по обеспечению достоверности, актуальности, конфиденциальности и целостности (сохранности) этих сведений
- обязанность работника по их соблюдению (выполнению)
- обязанность работника незамедлительно информировать службу ИБ о признаках некорректной работы или отказа цифровой медтехники, ИС и(или) о получении "подозрительных" сообщений
- обязанность работника хранить профессиональную тайну (пожизненно)

Использование мессенджеров

Запрет на использование **иностранных мессенджеров**

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

  - с 01.03.2023 - часть 8 ст. 10 закона № 149-ФЗ

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

Термины и определения (4)

Сайт в сети Интернет – совокупность программ для ЭВМ и иной информации, содержащейся в ИС, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети Интернет по доменным именам и(или) по сетевым адресам, позволяющим идентифицировать сайты в сети Интернет

Владелец сайта в сети Интернет – лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети Интернет и порядок размещения информации на сайте

Провайдер хостинга (сайта) – лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в ИС, постоянно подключенной к сети Интернет;
– обязательное уведомление об этом Роскомнадзора – включение в реестр провайдеров хостинга – с 01.12.2023. Предоставление хостинга без включения в реестр с 01.02.2024 запрещено !!

Операторы государственных ИС, ИС государственных (муниципальных) организаций должны использовать мощности российского провайдера хостинга, включенного в реестр, и **не вправе** использовать мощности, принадлежащие иностранным лицам – с 01.09.2024 !!

Запрет регистрации пользователей на российских сайтах с помощью аккаунтов в иностранных ИС, электронной почте (gmail.com) и т.п. – с 01.12.2023 !!

Авторизация пользователей в российских сайтах и ИС при доступе через Интернет – только с помощью: • ЕСИА, • ЕБС, • номера мобильного телефона, • иных ИС, соответствующих установленным требованиям защиты информации – с 01.12.2023 !!

[закон № 149-ФЗ в ред. от 31.07.2023]

Требования к сайтам медицинских организаций (1)

Обязательная публикация или ограничения на публикацию определенной информации, возможность направить сообщение владельцу сайта *etc*

- Гражданский кодекс РФ (часть 1), № 51-ФЗ от 30.11.1994 (ст. 152.1)
- О персональных данных, № 152-ФЗ от 27.07.2006
  ст.ст. 6, 9, 14, 18.1, 20 – публикация документов о политике обработки и защите персональных данных, получение согласия на их обработку *etc*
- Об информации, информационных технологиях и о защите информации, № 149-ФЗ от 27.07.2006 – ч. 2 ст. 10 – размещение "авторской" информации
- Об основах охраны здоровья граждан в РФ, № 323-ФЗ от 21.11.2011
  ст. 79 – публикация информации о медицинской организации, медработниках, сведений, необходимых для независимой оценки качества оказания услуг
- Об обязательном медицинском страховании в РФ, № 326-ФЗ от 29.11.2010
  пп. 6. 7 части 2 ст. 20
- О рекламе, № 38-ФЗ от 13.03.2006
- Правила предоставления медицинскими организациями платных медицинских услуг.
  – постановление Правительства РФ № 736 от 11.05.2023
  пп. 12–18, 42–44 – информация на сайте медорганизации

Медорганизация обязана опубликовать на своем сайте сведения о медицинских работниках:

- Ф.И.О., занимаемая должность
- сведения из документа об образовании: уровень образования, организация, выдавшая документ об образовании, год выдачи, специальность, квалификация
- сведения об аккредитации (сертификате) специалиста: специальность по занимаемой должности, срок действия
- график работы и часы приема медицинского работника

Согласие медработника **на публикацию** этих сведений **не требуется !!**
– ст. 79 закона № 323-ФЗ !

Требования к сайтам медицинских организаций (2)

- Об информации, необходимой для проведения независимой оценки качества оказания услуг медицинскими организациями, и требованиях к содержанию и форме предоставления информации об их деятельности, размещаемой на официальных сайтах (...) – приказ Минздрава РФ от 30.12.2014 № 956н
- Показатели, характеризующие общие критерии оценки качества условий оказания услуг медицинскими организациями (независимая оценка).
  – приказ Минздрава РФ от 04.05.2018 № 201н – критерии 1.1-1.3
- Рекомендации по предоставлению информации о деятельности медицинских организаций, размещаемой на официальных сайтах.
  – письмо Минздрава РФ от 15.03.2017 № 21-5/10/2-1757
- Порядок организации и оказания медицинской помощи с применением телемедицинских технологий. – приказ Минздрава РФ от 30.11.2017 № 965н – п. 46
- Порядок предоставления информации государственным (муниципальным) учреждением, ее размещения на официальном сайте в сети Интернет и ведения указанного сайта. – приказ Минфина РФ от 21.07.2011 № 86н
- Состав информации о результатах независимой оценки качества оказания услуг медицинскими организациями, – приказ Минфина РФ от 07.05.2019 № 66н

ГОСТ Р 52872-2012 Интернет-ресурсы. Требования доступности для инвалидов по зрению

мобильная версия

Самозапись.ру

горячая линия

8-343-385-03-03

Выберите регион

Свердловская обл.

Вход в личный кабинет

Вызов врача на дом

Запись на прием

Нельзя писать: "болен", "отпуск", "командировка"

Нет приема

Главная / Выбор поликлиники / Расписание

МУЗ "Детская городская больница №2 Поликлиническое отделение №2" г. Каменск-Уральский ул.Карла Маркса, д.50

Телефон: 8(3439)31-77-00

Врач	Пт 12 ноя	Сб 13 ноя	Вс 14 ноя	Пн 15 ноя	Вт 16 ноя	Ср 17 ноя	Чт 18 ноя	Пт 19 ноя	Сб 20 ноя	Вс 21 ноя	Пн 22 ноя
Специальность: Невролог											
Кузнецова Елена Владимировна	Нет расписания	Нет расписания	Выходной	12:00-18:00 Приемов:31	11:20-17:00 Приемов:31	09:00-14:00 Приемов:0	08:00-14:00 Приемов:31	Нет расписания	Нет расписания	Выходной	12:00-18:00 Приемов:31
Специальность: Отоларинголог											
Щелконогова Светлана Анатольевна	Нет расписания	14:10-17:45 Приемов:43	Выходной	Нет расписания	14:10-17:45 Приемов:43	Нет расписания	Нет расписания	14:10-17:45 Приемов:43	Выходной	Выходной	Нет расписания

Требования к сайтам – закон № 152-ФЗ

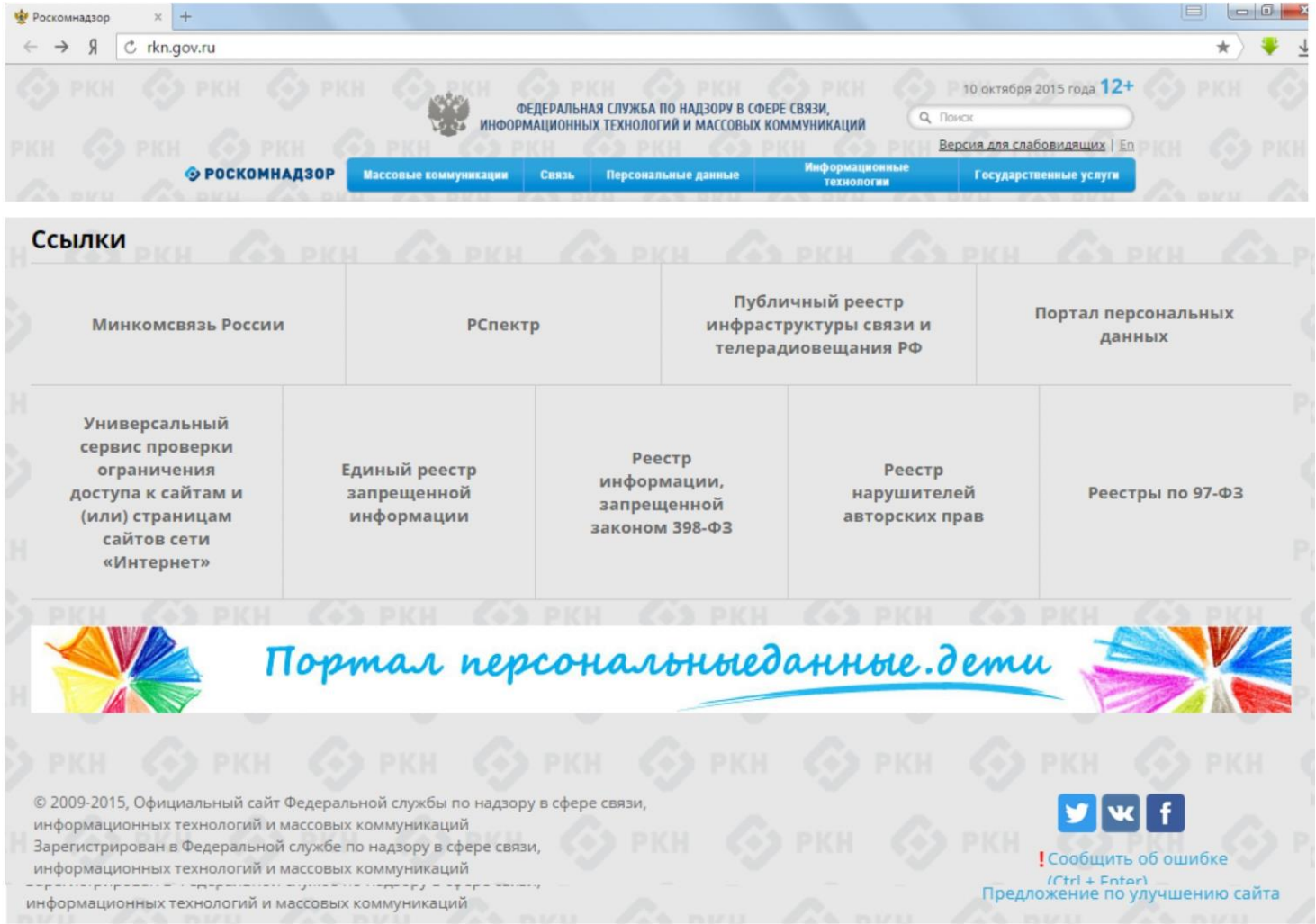
Владелец Интернет-сайта обязан:

- опубликовать на своем сайте документы, определяющие политику в отношении обработки персданных и реализации требований по их защите – ст. 18.1 !!
- предупредить пользователя, что передача данных по открытым каналам связи через сайт не гарантирует их конфиденциальность
- при необходимости предупредить пользователя об аутсорсинге обработки его персданных и получить его согласие на это + опубликовать сведения об аутсорсере на сайте – см. ст. 6 !!
- предупредить пользователя о применении cookies – цель, как они используются – получить его согласие, в случае отказа – предупредить о возможном изменении функциональности сайта
- получить согласие субъекта на распространение его персональных данных, разрешенных для распространения (при необходимости) – ст. 10.1 – см. приказ РКН от 24.02.2021 № 18

Предоставление пользователем своих персональных данных только после прочтения этих предупреждений -> получить согласие на их обработку на этих условиях:

- в форме договора присоединения – ст. 428 ГК РФ либо
- продолжить использовать сайт = факт дачи согласия (конклюдентные действия) либо
- продолжить использовать сайт без передачи персональных данных

Регламент ведения сайта медорганизации – ответственные – приказ !!



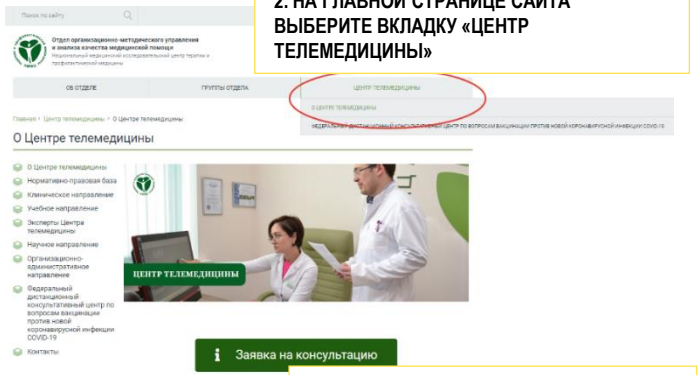
- Рекомендации Роскомнадзора от 21.09.2018 по защите личных персональных данных – **pd.rkn.gov.ru/docs/MR_itog**
- Разъяснения Роскомнадзора от 14.12.2012 по вопросам обработки персональных данных работников, соискателей на замещение вакантных должностей – **rkn.gov.ru/news/rsoc/news17877**
- Тест для оценки уровня правовой грамотности в вопросах обеспечения защиты своих персональных данных - **pd.rkn.gov.ru/docs/3**

Благодарю за внимание!

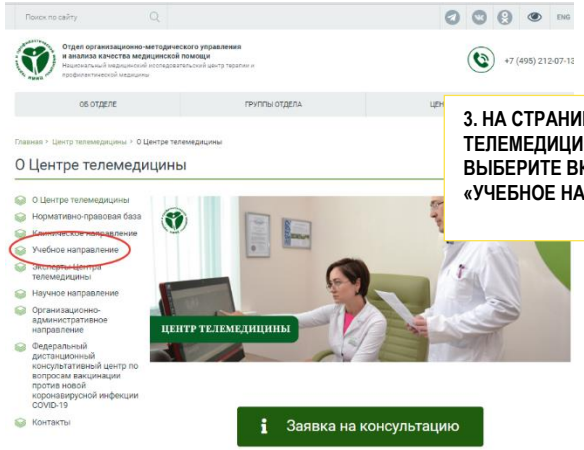
SOrlov@gnicpm.ru

Заполнение формы обратной связи

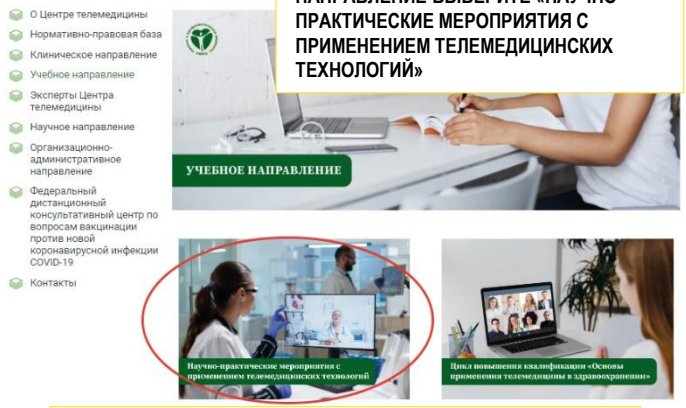
1. http://org.gnicpm.ru/



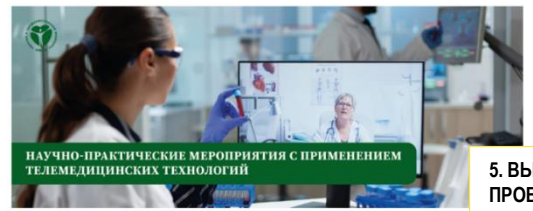
2. НА ГЛАВНОЙ СТРАНИЦЕ САЙТА ВЫБЕРИТЕ ВКЛАДКУ «ЦЕНТР ТЕЛЕМЕДИЦИНЫ»



3. НА СТРАНИЦЕ ЦЕНТРА ТЕЛЕМЕДИЦИНЫ ВЫБЕРИТЕ ВКЛАДКУ «УЧЕБНОЕ НАПРАВЛЕНИЕ»

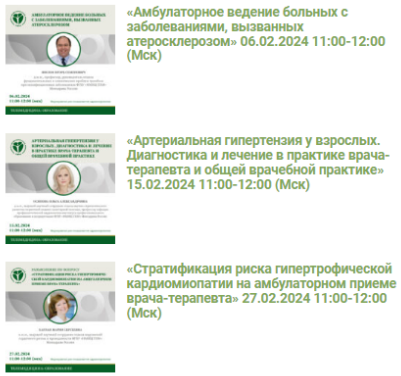


4. НА СТРАНИЦЕ УЧЕБНОЕ НАПРАВЛЕНИЕ ВЫБЕРИТЕ «НАУЧНО-ПРАКТИЧЕСКИЕ МЕРОПРИЯТИЯ С ПРИМЕНЕНИЕМ ТЕЛЕМЕДИЦИНСКИХ ТЕХНОЛОГИЙ»



5. ВЫБЕРИТЕ ГРАФИК ПРОВЕДЕНИЯ НАУЧНО-ПРАКТИЧЕСКИХ МЕРОПРИЯТИЙ

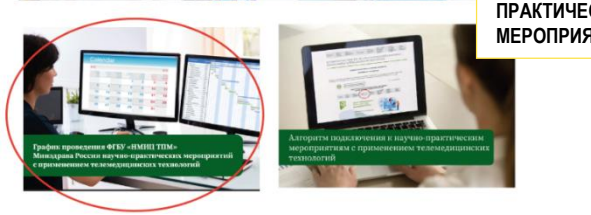
6. ВЫБЕРИТЕ ИНТЕРЕСУЮЩЕЕ ВАС МЕРОРОПРИЯТИЕ



«Амбулаторное ведение больных с заболеваниями, вызванных атеросклерозом» 06.02.2024 11:00-12:00 (Мск)

«Артериальная гипертензия у взрослых. Диагностика и лечение в практике врача-терапевта и общей врачебной практике» 15.02.2024 11:00-12:00 (Мск)

«Стратификация риска гипертрофической кардиомиопатии на амбулаторном приеме врача-терапевта» 27.02.2024 11:00-12:00 (Мск)



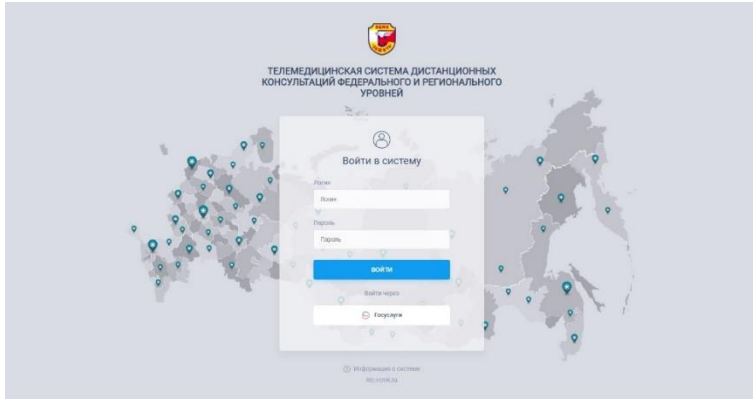
7. ЗАПОЛНИТЕ ФОРМУ ОБРАТНОЙ СВЯЗИ

Заявка на консультацию

Время работы

ПН	ВТ	Ср	ЧТ	ПТ	СБ	ВС
9:00-17:00 (мск)	9:00-17:00 (мск)	9:00-17:00 (мск)	9:00-17:00 (мск)	9:00-17:00 (мск)		

Кроме выходных и праздничных дней



Для подачи заявки на телемедицинскую консультацию необходимо быть зарегистрированным в Телемедицинской системе дистанционных консультаций федерального и регионального уровней (http://tmk.minzdrav.gov.ru/Account/Login).

Все актуальные материалы размещены на САЙТЕ Федерального дистанционного консультативного центра по вопросам вакцинации против новой коронавирусной инфекции COVID-19.

Вакцинация против новой коронавирусной инфекции COVID-19. Лучшие региональные практики

Федеральный дистанционный консультативный центр по вопросам вакцинации против новой коронавирусной инфекции COVI-19 создан с целью:

- консультативной помощи с применением телемедицинских технологий по вопросам вакцинации против новой коронавирусной инфекции COVID-19;
- проведения еженедельных дистанционных семинаров «Региональный опыт организации проведения вакцинации против новой коронавирусной инфекции COVID-19»;
- информирования населения по телефонам «горячей линии» по вопросам вакцинации против новой коронавирусной инфекции COVID-19.

Телефон горячей линии: +7 (495) 790-71-72

Обращаем ваше внимание, что ФГБУ «НМИЦ Терапии и Профилактической медицины» Министерства здравоохранения Российской Федерации оказывает медицинскую помощь с применением телемедицинских технологий по профилю Терапия и Терапия (COVID-19 вакцинация) пациентам достигших возраста **18 лет.**

+7 (499) 553-69-19

org.gnicpm.ru

telemed@gnicpm.ru

СПАСИБО ЗА ВНИМАНИЕ!

ФГБУ «НМИЦ ТПМ» Минздрава России

Наши контакты:

Москва, Петроверигский пер., д. 10, стр. 3

Москва, Китайгородский пр., д. 7

+7 (495) 790-71-72

vk.com/gnicpmru

www.gnicpm.ru

t.me/fgbunmictpm