Защита медицинских данных
Риски, правила, решения

ЕМП

Цифровые сервисы здоровья

Далее

ПРЕЗЕНТАЦИЯ ДЛЯ Вебинара Компании ЕМП 05.06.25 г.

Спикеры вебинара

Андрей Трунов
Директор по развитию бизнеса Компания ЕМП

Александр Бодров
Руководитель направления аналитического отдела АО «ИнфоТеКС»

План вебинара

Что изменилось в законах — и как это влияет на медицинские учреждения
Почему ИТ-контур медицинских учреждений под прицелом и где нельзя рисковать
Какие каналы коммуникаций запрещены, как выстроить защиту данных правильно
Что требует КИИ и как избежать утечки персональных данных

001

Контекст

О важных изменения
в законодательстве

002

Решение

Как выстроить защищенный
ИТ-контур

003

Требования и риски

Чем грозит не соблюдения
требований законодательства

004

Вопросы и преимущества

Ответы на вопросы и демонстрация
преимуществ платформы

Анализ рисков утечки ПДн

Риски

- Идентифицирующие данные
- Медицинская информация
- Финансовые данные
- Личная информация

Угрозы

- Ценность данных
- Внутренние угрозы
- Социальная инженерия
- Технические уязвимости
- Физическое воздействие

В современном мире медицинские данные становятся все более цифровыми, что создает дополнительные угрозы их безопасности. Рост телемедицины, электронных медицинских карт и систем хранения данных увеличивает вероятность утечек

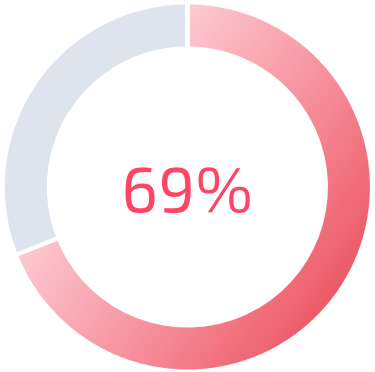
Последствия утечки

Репутационные риски	Потеря доверия пациентов
Финансовые потери	Оформление кредитов, мошенничество со страховками
Психологический ущерб	Шантажирование, дискриминация
Юридические последствия	Штрафы, уголовная ответственность

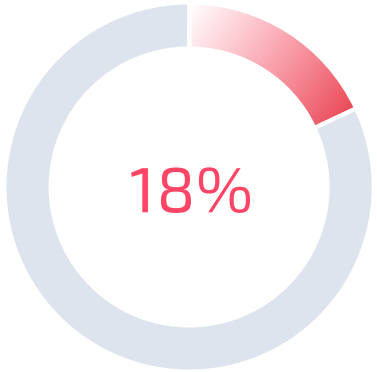
Защита медицинских ПДн требует комплексного подхода и постоянного внимания к безопасности

Нет права на ошибку

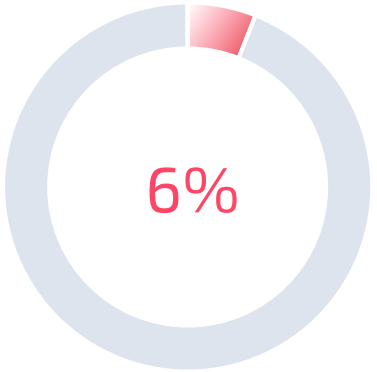
Как изменится ваше отношение к компании, допустившей утечку ваших персональных данных?



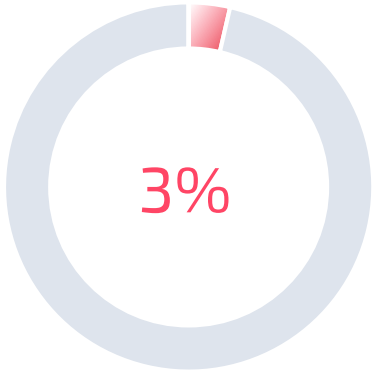
Больше не буду пользоваться услугами этой компании



Перейду к конкурентам, если их предложения не уступают по цене и качеству



Напишу негативный отзыв, но продолжу пользоваться



Продолжу пользоваться услугами этой компании, меня все устраивает

*Данные companies.rbc.ru

Кодекс Российской Федерации об административных правонарушениях

Статья 13.11 Нарушение законодательства Российской Федерации в области персональных данных

- **ч. 16:** Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей специальную категорию персональных данных.

Статья 13.11.2 Незаконное использование принадлежащих иностранным юридическим лицам и (или) иностранным гражданам информационных систем и (или) программ для электронных вычислительных машин

Статья 13.12 Нарушение правил защиты информации

- **ч. 6** нарушение требований о защите информации, установленных федеральными законами и принятыми в их исполнение НПА.

Статья 13.12.1 Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

- **ч.1** Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат признаков уголовно наказуемого деяния.

Статья 13.14 Разглашение информации с ограниченным доступом

Уголовный кодекс Российской Федерации

Статья 137 Нарушение неприкосновенности частной жизни

Статья 272.1 Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения

Статья 274 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Статья 274.1 Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

ГИС

КИИ

ИСПДн

Безопасность ГИС

149 ФЗ

Постановление Правительства РФ от 06.07.2015 N 676
«О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»

Приказ **ФСБ** России от 18.03.2025 № 117
"Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств"

Приказ **ФСТЭК** России от 11.02.2013 № 17
«Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Приказ ФСБ России от 18.03.2025 № 117

Уровень значимости информации	Масштаб ИС (Сегмента ИС)		
	ИС (сегмент ИС), предназначенная для решения задач ИС на всей территории РФ или в пределах 2-х и более субъектов РФ	ИС (сегмент ИС), предназначенная для решения задач ИС в пределах одного субъекта РФ	ИС (сегмент ИС), предназначенная для решения задач ИС в пределах гос.органа, муниципал. обр. и/или организации
Высокий	КВ	КС3	КС2
Средний	КС3	КС3	КС1
Низкий	КС2	КС1	КС1

Безопасность ПД в ИСПДн

152 ФЗ

Постановление Правительства РФ от 01.11.2012 № 1119
«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Приказ **ФСБ** России от 10.07.2014 № 378
«Об утверждении Состава и содержания организационных и технических мер…»

Приказ **ФСТЭК** России от 18.02.2013 № 21
«Об утверждении Состава и содержания организационных и технических мер…»

Статья 19 152-ФЗ. Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации

КИИ 187-ФЗ от 26 июля 2017 г.

Статья 2

субъекты критической информационной инфраструктуры - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

ЕМП

Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Пункт 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):

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

б) создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение.

Пункт 6

Установить, что с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

ЕМП

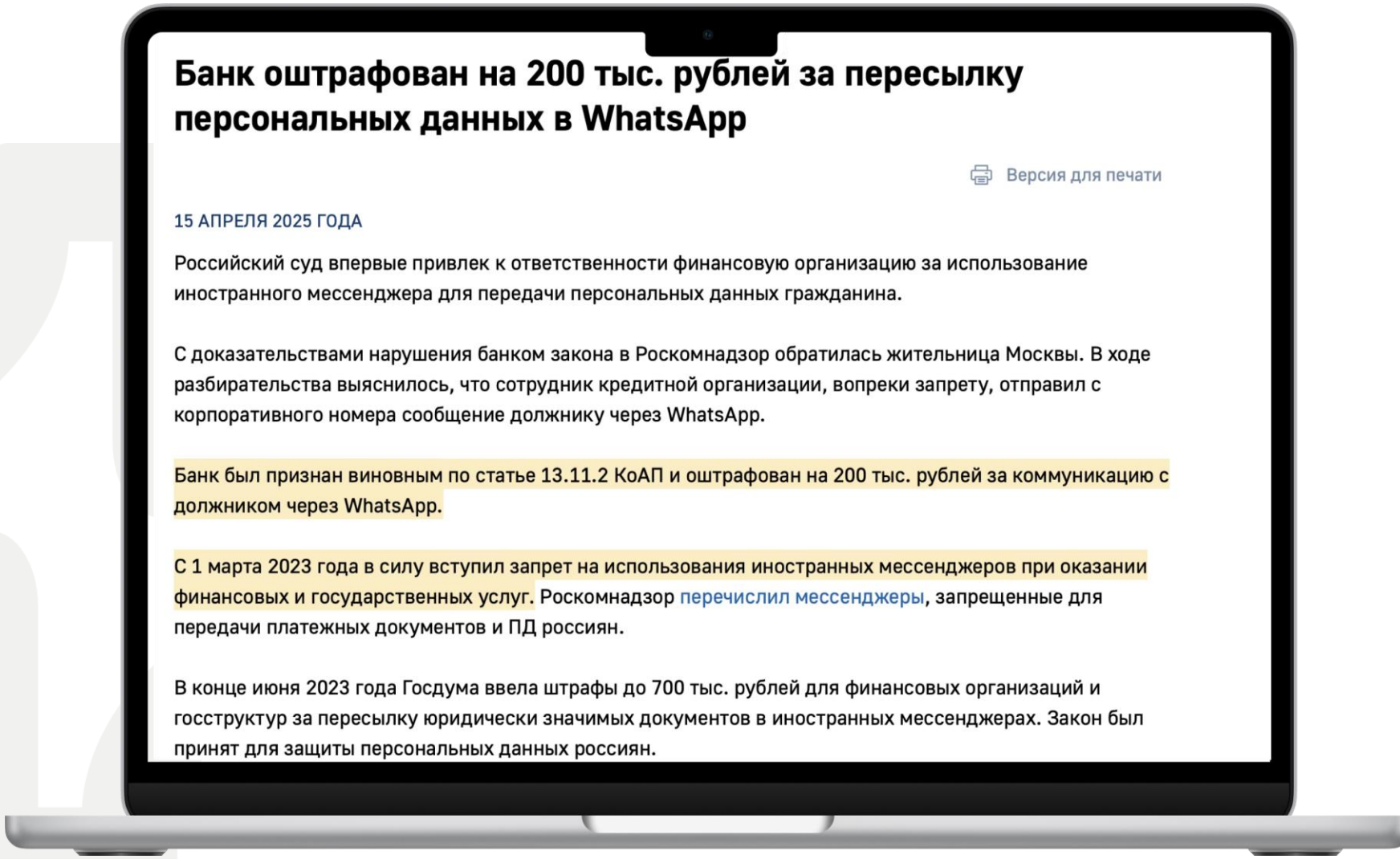
Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»

Пункт 1

с 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 г. N 223-ФЗ не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования на принадлежащих им значимых объектах КИИ Российской Федерации, а также закупки услуг, необходимых для использования этого программного обеспечения на таких объектах, без согласования возможности осуществления закупок с федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации, или с Центральным банком Российской Федерации (в соответствии с его полномочиями, установленными законодательством Российской Федерации);

Прецедент!

РОСКОМНАДЗОР



Банк оштрафован на 200 тыс. рублей за пересылку персональных данных в WhatsApp

Версия для печати

15 АПРЕЛЯ 2025 ГОДА

Российский суд впервые привлек к ответственности финансовую организацию за использование иностранного мессенджера для передачи персональных данных гражданина.

С доказательствами нарушения банком закона в Роскомнадзор обратилась жительница Москвы. В ходе разбирательства выяснилось, что сотрудник кредитной организации, вопреки запрету, отправил с корпоративного номера сообщение должнику через WhatsApp.

Банк был признан виновным по статье 13.11.2 КоАП и оштрафован на 200 тыс. рублей за коммуникацию с должником через WhatsApp.

С 1 марта 2023 года в силу вступил запрет на использования иностранных мессенджеров при оказании финансовых и государственных услуг. Роскомнадзор перечислил мессенджеры, запрещенные для передачи платежных документов и ПД россиян.

В конце июня 2023 года Госдума ввела штрафы до 700 тыс. рублей для финансовых организаций и госструктур за пересылку юридически значимых документов в иностранных мессенджерах. Закон был принят для защиты персональных данных россиян.

Делать

Не делать

710 млн записей за 2024 год

Риски растут: кибератаки становятся сложнее, а хакеры — умнее
Используют ИИ и атакуют не только данные, но и инфраструктуру

По данным компании «Перспективный мониторинг» (ГК «ИнфоТеКС») в мае 2025 года зафиксирована утечка 1,5 млн записей и 4,2 тыс. документов в сфере медицины

Такого прецедента не было

Никогда ранее
в истории
не публиковалось
столько данных
одновременно

Атаки второй половины 2024 года

ВГТРК
Dr.Web
Банки и ВЭФ
Центр ЭП
Операторы связи

Утечек за год

135

зафиксировал
Роскомнадзор
в течении 2024 года

Одна утечка

500 млн

Самый крупный инцидент
Чья база — не раскрыто

КИБЕРУГРОЗЫ СТАНОВЯТСЯ РЕАЛЬНОЙ ОПАСНОСТЬЮ

Ужесточение наказания

30 ноября 2024 года президент России Путин В.В. подписал федеральный закон № 421-ФЗ, вводящий уголовную ответственность за незаконные использование, передачу, сбор и хранение персональных данных граждан
Максимальное наказание за подобные преступления составляет до 10 лет лишения свободы

До принятия закона подобные нарушения квалифицировались по статье 137 УК РФ «Нарушение неприкосновенности частной жизни», либо влекли административную ответственность
Новый закон значительно расширяет перечень наказуемых деяний и ужесточает санкции за противоправные действия с персональными данными граждан

Для должностных лиц

30 тыс.
до 50 тыс.

Для юридических лиц

100 тыс.
до 700 тыс.

Федеральный закон от 24 июня 2023 г. № 277-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях" был подписан Президентом РФ, опубликован и вступил в силу 24 июня 2023 года

Законом вводится новая ст. 13.11.2 КоАП в соответствии с которой за незаконное использование иностранных мессенджеров установлен административный штраф

Ответственность

К объектам защиты медицинской информационной системы относят

сведения в базе данных
резервные и архивные копии сервера
целевые данные администратора и начальника
средства обеспечения функционирования медицинской информационной системы
обработка информации в медучреждении – сбор, хранение, передача
производительность файлового сервера

Согласно части 1 статьи 10 закона №152-ФЗ персональные данные, касающиеся состояния здоровья, относятся к специальной категории персональных данных

Вероятные угрозы

Задача по организации безопасной обработки и хранения медицинских данных пациентов всегда стоит перед главным врачом и входит в его зону ответственности

Юридические лица

Предусмотрен оборотный штраф за повторную утечку данных в размере от 1% до 3% от годовой выручки

Минимальная сумма взыскания составит 20 млн. рублей, максимальная 500 млн. рублей

Должностные лица

Предусмотрен штраф при утечке персональных данных до 2 млн. рублей

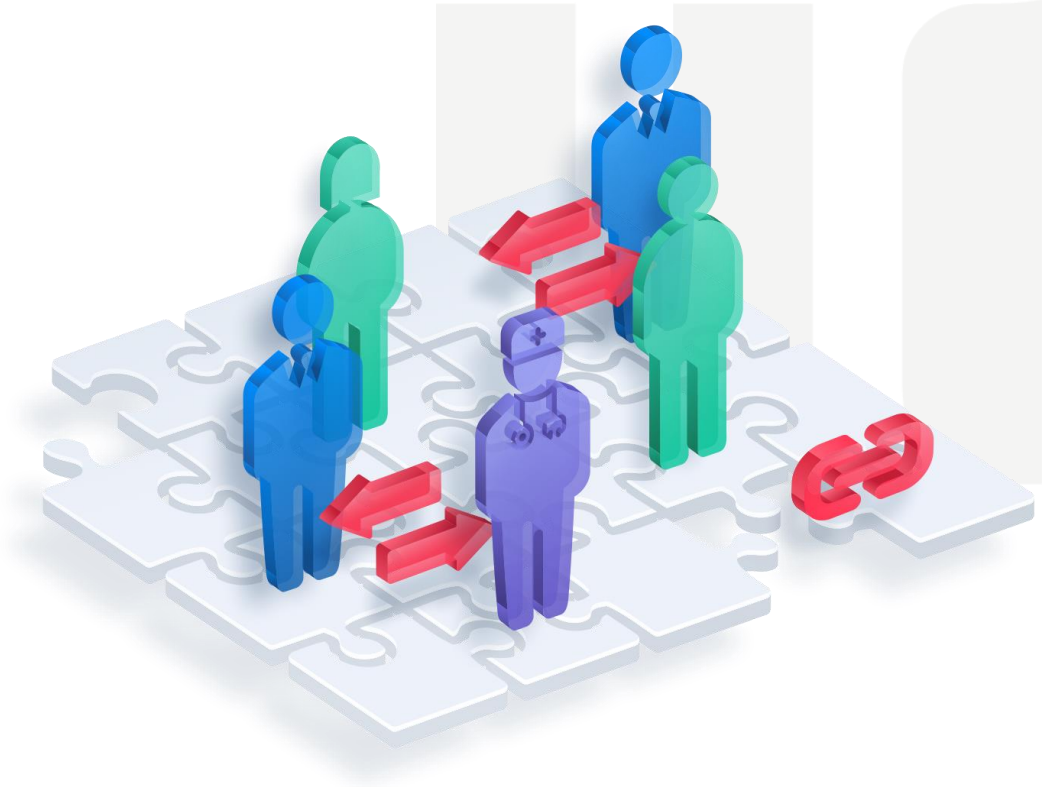
При повторной утечке в серьезных случаях запрет на занятие профессиональной деятельностью до 5 лет или лишение свободы на срок до 4 лет

Запрет на использование иностранных мессенджеров для ряда российских организаций вступил в силу с 1 марта 2023 года (ч. 8 ст. 10 Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации")

Запрещенные мессенджеры

Discord
Microsoft Teams
Skype for Business
Snapchat
Telegram
Threema
Viber
WhatsApp
WeChat

Запрет на использование иностранных мессенджеров



При предоставлении государственных и муниципальных услуг

При выполнении государственного или муниципального задания

При реализации товаров, работ, услуг, имущественных прав

Для передачи платежных документов или предоставления информации, содержащей персональные данные граждан РФ

Компания обладает многолетней уникальной экспертизой в области цифровизации учреждений здравоохранения

Компания ЕМП – кто мы?

Российский разработчик и поставщик цифровых продуктов

Платформа ЕМП-здоровье – собственная разработка, является ИИС, подключена к ЕГИСЗ

Компания ЕМП входит в ГК «ИнфоТеКС» – одного из лидеров рынка информационной безопасности РФ

С платформой «ЕМП-здоровье» ваша клиника:

Увеличит охват рынка клиентов

Расширит свою географию присутствия без открытия дополнительных филиалов

Запустит новый перспективный канал продаж

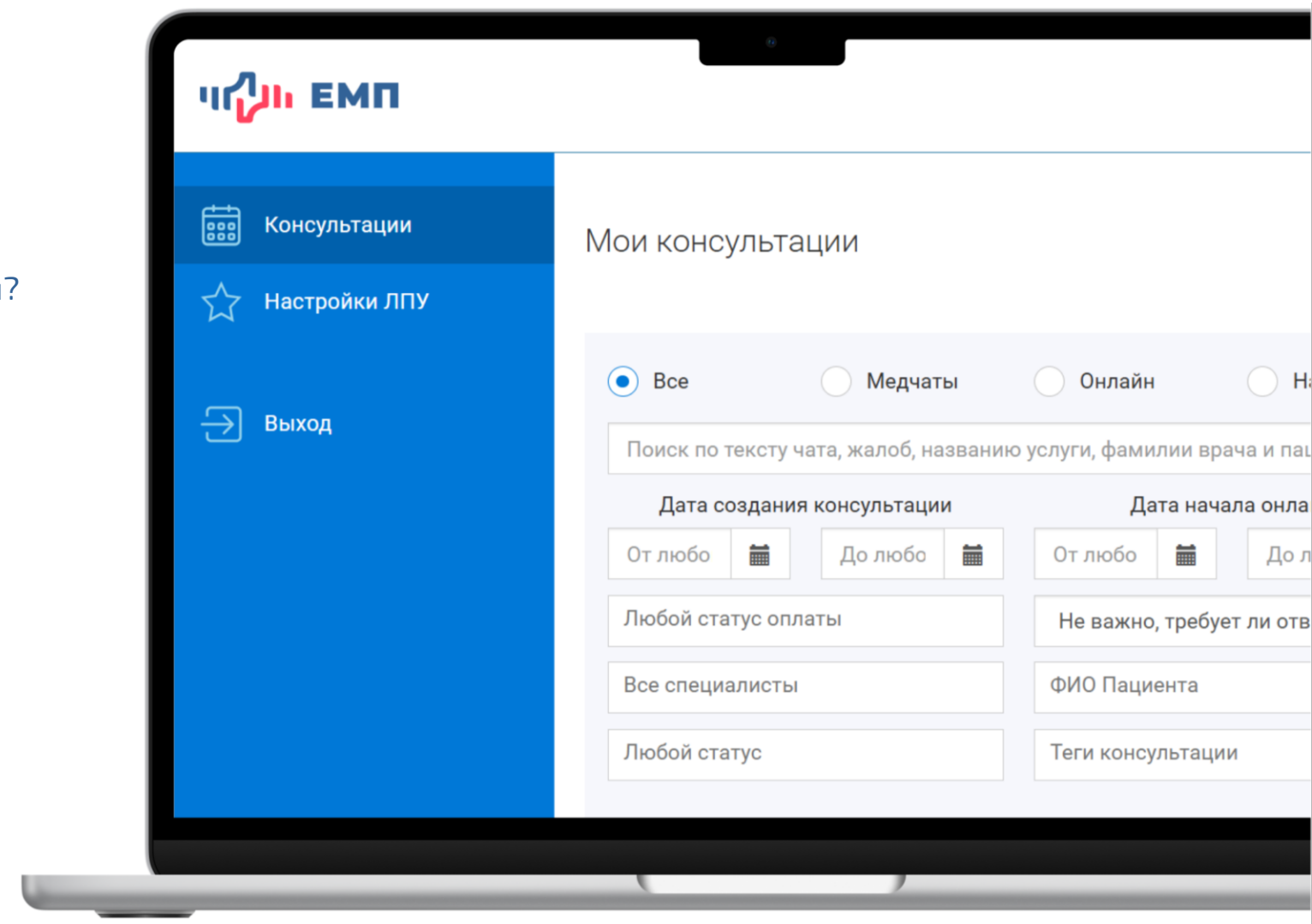
Станет привлекательным партнером для страховых компаний

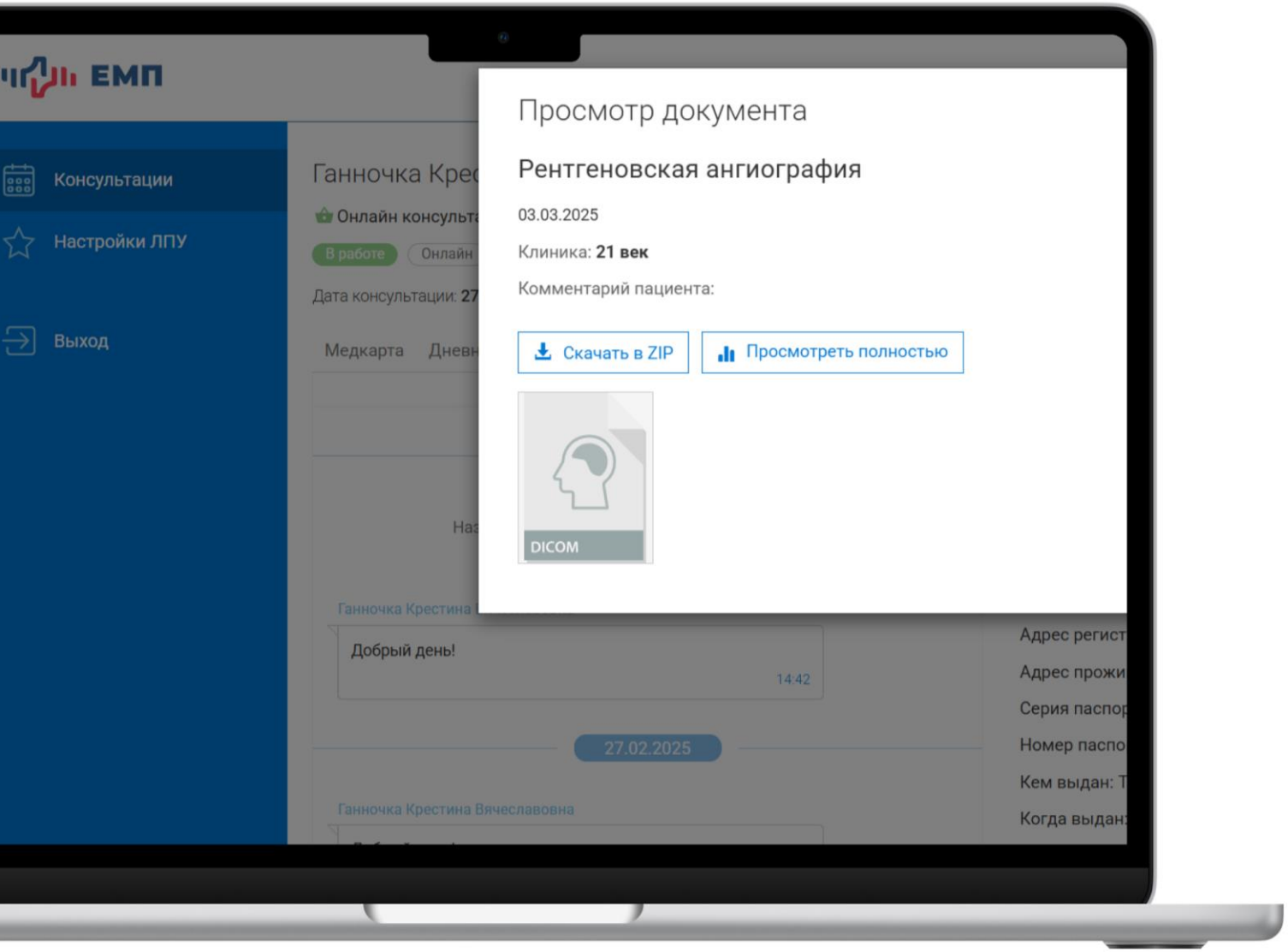
Готовое решение «ЕМП-здоровье»

Какие услуги клиника может оказывать онлайн?

- Консультации специалистов
- Сопровождение пациентов с хроническими заболеваниями/после операций
- Мониторинг показателей здоровья
- Второе мнение
- Запись на прием к врачу
- Дистанционные программы реабилитации
- Отбор пациентов на лечение, в т.ч. на ВМП
- Телемедицинские консультации врач-врач
- Консилиумы и др.

Платформа создана для клиник и врачей, которые дорожат своей репутацией и стремятся соблюдать требования законодательства





Работа с документами и подписями

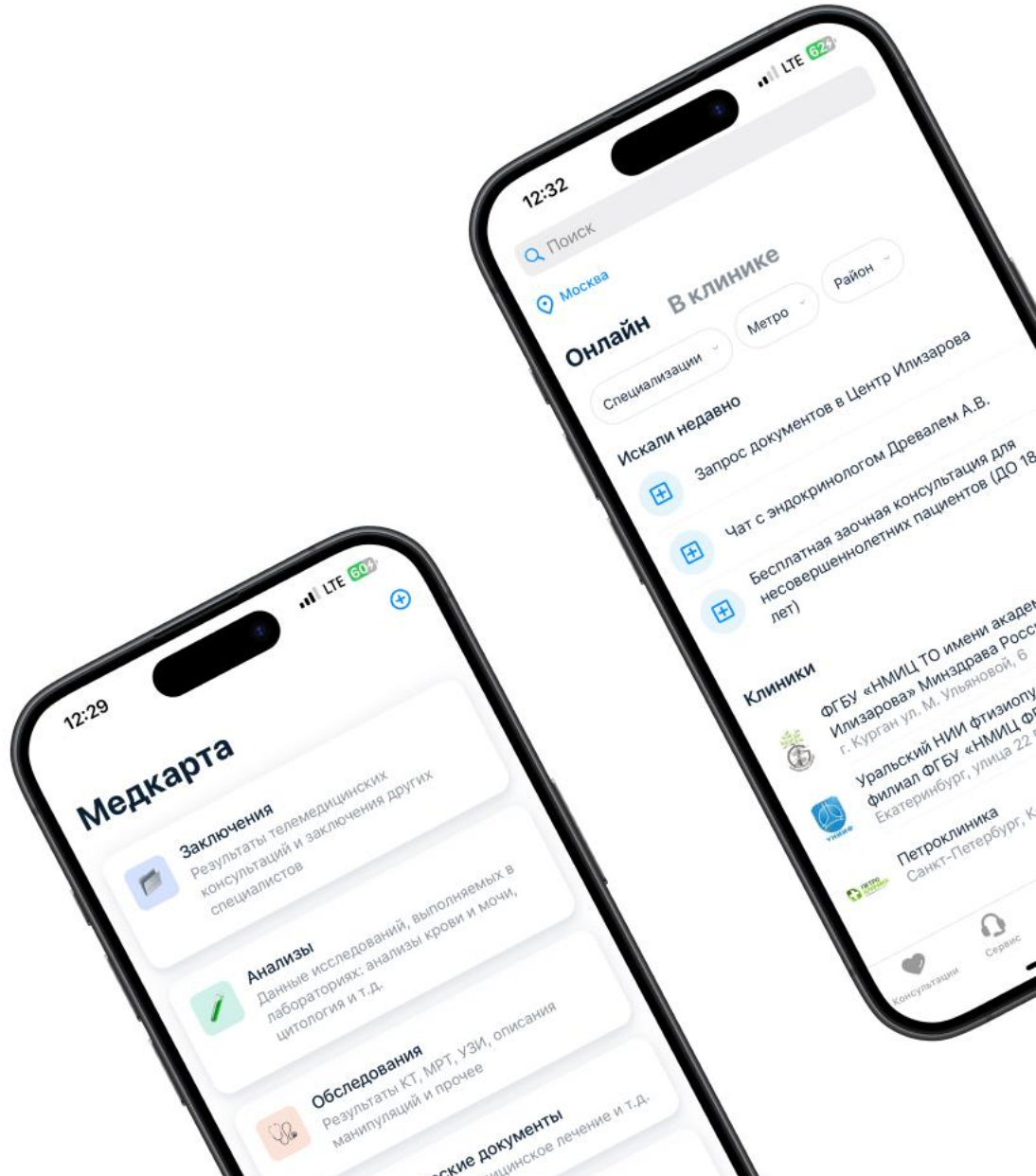
- Пациенту доступна авторизация через ЕСИА или по номеру телефона
- Пациент акцептирует нужные документы (Согласие на обработку персональных данных, условия оказания услуги и ИДС)
- Врач использует электронную подпись для подписания консультативных заключений и ИДС

Документы медкарты доступны врачу и надежно защищены (долговременное хранение документов, в т.ч. радиологических изображений DICOM)

Настройте платформу «ЕМП-здоровье» под задачи вашей клиники

- Управляйте профилями клиники и врачей
- Настраивайте услуги (тип, стоимость, продолжительность и другие параметры)
- Добавляйте расписания врачей и услуг (интеграция с МИС)
- Управляйте заявками от пациентов через пульт (маршрутизация и контроль)
- Настраивайте фильтры и формируйте отчеты по нужным критериям
- Добавляйте свои шаблоны (консультативные заключения, опросники для пациентов и пр.)
- Настраивайте специальные визарды заказа услуг и берите в работу готовые заявки (пациент при заказе услуги сразу загрузит нужные врачу документы и ответит на вопросы)

Общайтесь с пациентами в надежном защищенном специализированном мессенджере

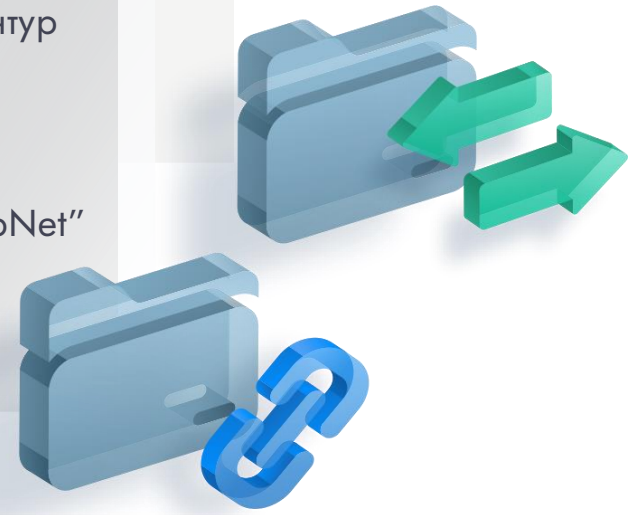


Защита данных на платформе

Данные хранятся в российском дата-центре

Передача и хранение медицинских данных организованы по классу К2 в соответствии с 152-ФЗ.

Защищенный контур безопасности и программное обеспечение “VipNet” на базе решений «ИнфоТеКС»



Техническая поддержка платформы осуществляется специалистами по информационной безопасности: регулярные обновления и настройка

Кейс

медицинский исследовательский центр (ФГБУ)

Запрос бизнес-заказчика

Конфигурация «Заочные консультации по травматологии и ортопедии» должна обеспечивать возможность организации и проведения платных и бесплатных заочных консультаций с возможностью загрузки перечня необходимых документов, включая радиологические изображения в формате DICOM, с последующей записью пациентов на госпитализацию

Цель :

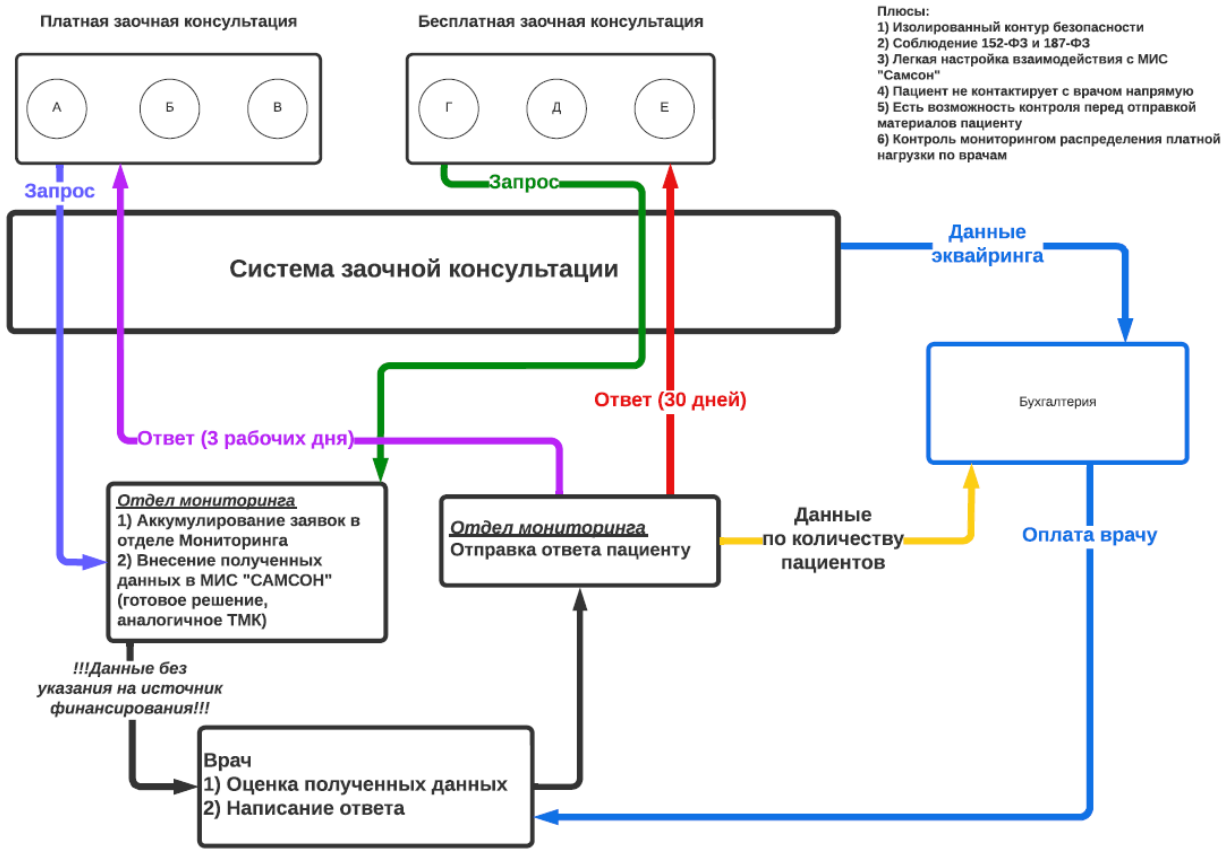
отбор пациентов на лечение и определение источника финансирования этого лечения

Договорная база :

- лицензионный договор на получение неисключительного права использования платформы «ЕМП-здоровье»
- договор на услуги по донастройке платформы «ЕМП-здоровье»
- договор на техническую поддержку платформы «ЕМП-здоровье»

Срок реализации :

2 месяца



Цифровизация дистанционных обращений

Задача

Структурировать поток обращений и ускорить их обработку при соблюдении требований ИБ и 152-ФЗ

Решение

Разработали и внедрили цифровой сервис дистанционного консультирования с авторизацией через ЕСИА, техподдержкой и системой отчетности

Функциональность

Бесплатные и платные заочные консультации

Видео-консультации «пациент-врач»

Прием полного пакета документов

Формирование отчетов по обращениям

Результат

После ряда встреч и демонстраций на основании запросов и экспертных рекомендаций отдела разработки компании ЕМП, было создано техническое задание для реализации проекта. Работы были произведены в течении 2 месяцев.

Результат работы

На данный момент Центр расширяет номенклатуру дистанционных услуг для решения следующих задач:

Консультация по результатам лечения (контрольные исследования направляются лечащему врачу)
Запрос документов пациентами, которые получали лечение в Центре

1000+

Консультаций в месяц

500 000 тыс. руб.

Средний ежемесячный оборот по платным услугам Центра

Сайт

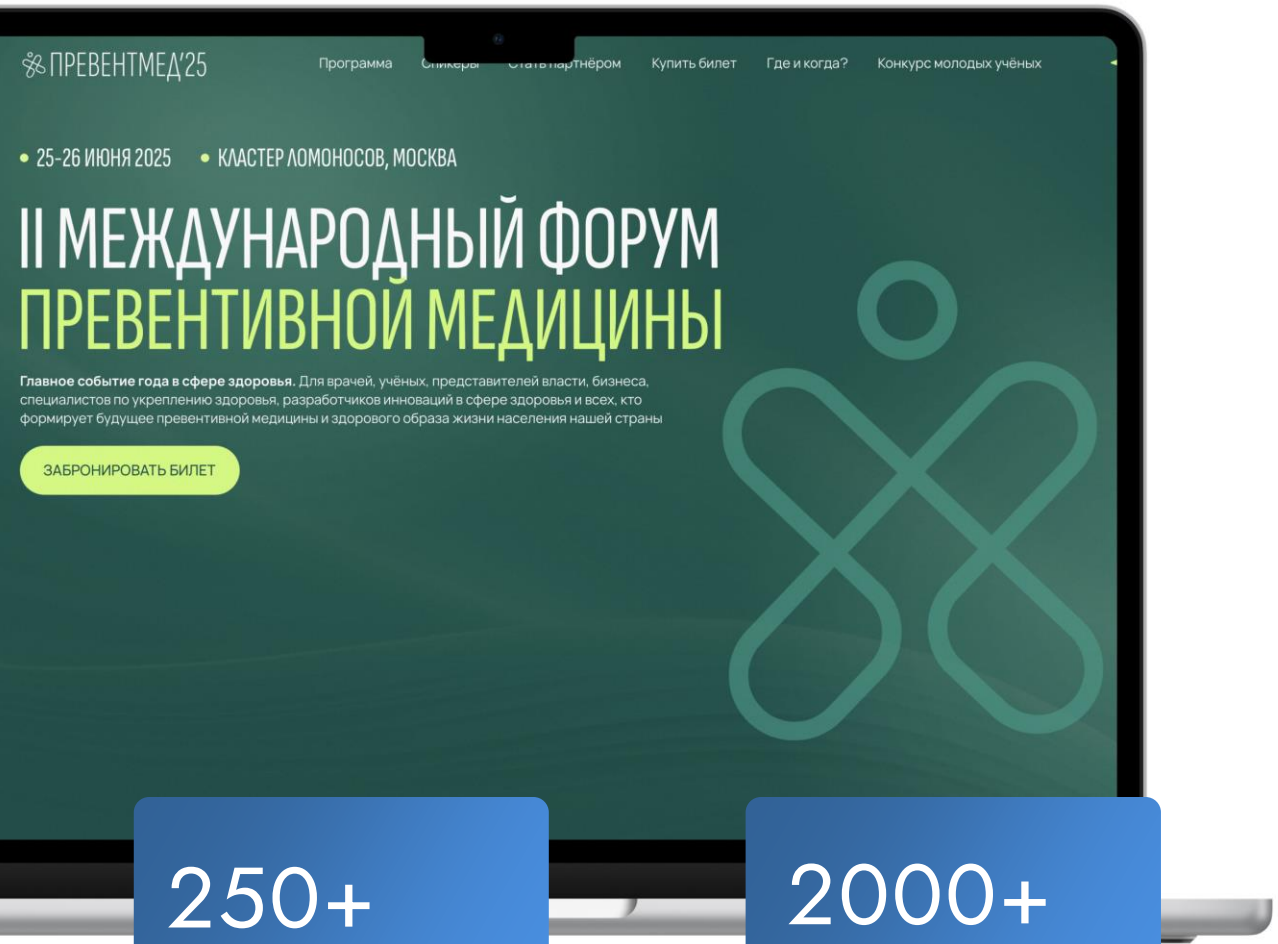
Промокод

ЕМП

ПРЕВЕНТМЕД'25

Мы дарим участникам промокод - ЕМП

-15% на участие во II Международном форуме превентивной медицины — главном событии в сфере медицины 2025 года



250+
Спикеров

2000+
Участников

ПРЕВЕНТМЕД'25

Организатор мероприятия – ФГБУ «Национальный медицинский исследовательский центр терапии и профилактической медицины» Министерства здравоохранения Российской Федерации в партнерстве с ФГБНУ РНЦХ им. акад. Б.В. Петровского

Форум соберет представителей законодательной и исполнительной власти федерального и регионального уровня, ведущих российских и зарубежных экспертов и лидеров мнения, представителей научных медицинских исследовательских центров, государственных и частных медицинских организаций, и бизнеса

Компания ЕМП является модератором круглого стола сессии "Защита медицинских данных. Риски, правила, решения"

На круглом столе будут обсуждаться ключевые вызовы в сфере обработки специальных категорий персональных данных в условиях цифровизации здравоохранения, риски и последствия утечек, вопросы повышения доверия пациентов к цифровым сервисам

Сайт

Кодовое слово

ВЕБИНАР

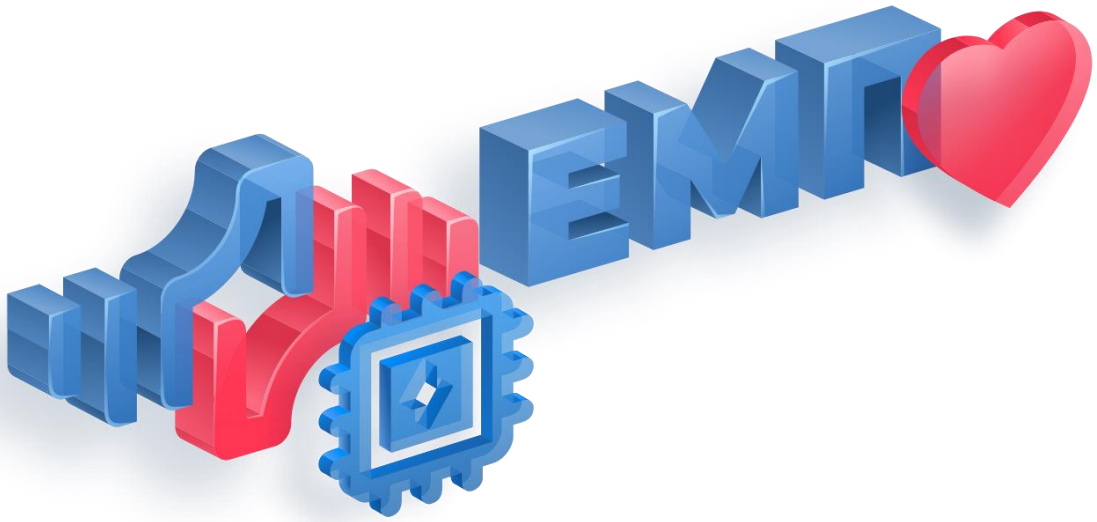
Демонстрация платформы «ЕМП – здоровье»

Приглашаем участников на бесплатную демонстрацию платформы «ЕМП-здоровье»

Первым 20 обратившимся -15% на услуги подключения платформы

*При заполнении заявки на сайте в тексте обращения необходимо указать кодовое слово «ВЕБИНАР»

Благодарим за внимание



Контакты 8 800 5555 782 info@emp-health.ru http://emp-health.ru