ФМБА РОССИИ
Федеральное медико-биологическое агентство

Федеральное государственное бюджетное учреждение
«Государственный научный центр Российской
Федерации – Федеральный медицинский
биофизический центр имени А.И. Бурназяна»
Федерального медико-биологического агентства

Романова Т.Е., Бердутин В.А., Абаева О.П.

ВРАЧ КАК ЦИФРОВОЙ ЛИДЕР

Методическое пособие

Москва, 2025

Федеральное медико-биологическое агентство
Федеральное государственное бюджетное учреждение
«Государственный научный центр Российской Федерации –
Федеральный медицинский биофизический центр
имени А.И.Бурназяна»
МЕДИКО-БИОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ
ИННОВАЦИЙ И НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ

Романова Т.Е., Бердутин В.А., Абаева О.П.

ВРАЧ КАК ЦИФРОВОЙ ЛИДЕР

Методическое пособие

Москва 2025

УДК 614.39
ББК 51.1
Р69

Романова Т.Е., Бердутин В.А., Абаева О.П.
Врач как цифровой лидер. Методическое пособие — М.: ФГБУ ГНЦ ФМБЦ им. А.И. Бурназяна ФМБА России, 2025. — 62 с.

Авторы:

Романова Татьяна Евгеньевна — к.м.н., доцент, заведующий кафедрой общественного здоровья и здравоохранения Федерального государственного бюджетного образовательного учреждения высшего образования "Приволжский исследовательский медицинский университет" Министерства здравоохранения Российской Федерации

Бердутин Виталий Анатольевич — к.м.н., доцент кафедры выездного и инновационного обучения по интегрированным дисциплинам МБУ ИНО ФГБУ ГНЦ ФМБЦ им. А.И. Бурназяна ⑲⑪—◠⑮588⑲⑨)

Абаева Ольга Петровна — д.м.н., доц., профессор кафедры социологии медицины, экономики здравоохранения и медицинского страхования ФГАОУ ВО Первый МГМУ им. ⑦.⑪. Сеченова, профессор кафедры выездного и инновационного обучения по интегрированным дисциплинам МБУ ИНО ФГБУ ГНЦ ФМБЦ им. А.И. Бурназяна ⑲⑪—◠⑮588⑲⑨)

Рецензенты:

Манерова Ольга Александровна — профессор кафедры общественного здоровья и здравоохранения им. Н.А. Семашко Федерального государственного автономного образовательного учреждения высшего образования Первый Московский государственный медицинский университет имени И.М. Сеченова Министерства здравоохранения Российской Федерации (Сеченовский Университет)

Кром Ирина Львовна — профессор кафедры общественного здоровья и здравоохранения (с курсами правоведения и истории медицины) Федерального государственного бюджетного образовательного учреждения высшего образования «Саратовский государственный медицинский университет имени В.И. Разумовского» Министерства здравоохранения Российской Федерации

Врач сегодня — это не только специалист в области диагностики и лечения, активный участник цифровых процессов, но и цифровой лидер. От его способности адаптироваться к новым технологиям, соблюдать нормы информационной безопасности и использовать цифровые ресурсы зависит не только эффективность его работы, но и доверие больных и коллег. Цифровое лидерство врача подразумевает не только использование технологий, но и способность быть проводником изменений, обучать других, а также активно участвовать в развитии цифровой экосистемы здравоохранения, где особую важность приобретают вопросы защиты врачебной тайны и персональных данных пациентов, которые в условиях цифровизации становятся более уязвимыми. Настоящее пособие нацелено на решение упомянутых проблем и может служить руководством для врачей всех специальностей, которые намерены развивать и совершенствовать свои цифровые навыки и компетенции.

ISBN 978-5-93064-396-1

Содержание

ВВЕДЕНИЕ

Современная медицина находится на этапе активной цифровой трансформации, которая затрагивает все аспекты отечественного здравоохранения. Внедрение цифровых технологий, таких как электронные медицинские карты, телемедицина, системы анализа больших данных и искусственный интеллект, открывает новые возможности для повышения качества медицинской помощи, оптимизации работы врачей и улучшения взаимодействия с пациентами. Однако эти изменения требуют от медицинских специалистов не только профессиональных знаний, но и цифровой грамотности, умения эффективно использовать современные инструменты и платформы.

Врач сегодня — это не только специалист в области диагностики и лечения, но и активный участник цифровых процессов. От его способности адаптироваться к новым технологиям, соблюдать нормы информационной безопасности и использовать цифровые ресурсы зависит не только эффективность его работы, но и доверие пациентов. Особую важность приобретают вопросы защиты врачебной тайны и персональных данных пациентов, которые в условиях цифровизации становятся более уязвимыми.

Цифровое лидерство врача подразумевает не только использование технологий, но и способность быть проводником изменений, обучать коллег и пациентов, а также активно участвовать в развитии цифровой экосистемы здравоохранения. Данное методическое пособие призвано помочь врачам стать уверенными цифровыми лидерами, способными эффективно работать в новых условиях.

Именно по этой причине основной целью методического пособия является предоставление врачам практических знаний и навыков, необходимых для успешной работы в условиях цифровой трансформации отечественного здравоохранения. Пособие направлено на развитие цифровой грамотности, понимание современных технологий и их применения в медицинской практике, а также на формирование ответственного подхода к использованию цифровых инструментов.

Задачи, которые решает настоящее методическое пособие:

- Ознакомление врачей с современными средствами коммуникации (электронная почта, мессенджеры и т. д.), а также с правилами их использования с учетом соблюдения врачебной тайны.
- Изложение способов защиты каналов связи и важности использования безопасных методов передачи данных.
- Объяснение принципов использования электронной цифровой подписи и ее применения в медицинской практике.
- Ознакомление врачей с предназначением и основными возможностями Единой государственной информационной системы здравоохранения (ЕГИСЗ), портала Госуслуг и Единой системы идентификации и аутентификации (ЕСИА).
- Демонстрация эффективного использования цифровых инструментов для повышения качества и доступности медицинской помощи, а также для оптимизации производственных процессов учреждений здравоохранения.
- Объяснение важности соблюдения принципов цифровой этики в деле защиты персональных данных пациентов.

ГЛАВА 1. СОВРЕМЕННЫЕ СРЕДСТВА КОММУНИКАЦИИ В МЕДИЦИНЕ

В данной главе предлагаются краткое описание и четкие инструкции по безопасному и разумному использованию электронной почты, мессенджеров и других коммуникационных инструментов, а также подчеркивается их связь с проблемами при соблюдении врачебной тайны и перспективами интеграции в цифровую экосистему отечественного здравоохранения.

Электронная почта: безопасность, этикет и врачебная тайна

Электронная почта давно стала неотъемлемой частью профессиональной коммуникации, в том числе в медицине. Она позволяет быстро обмениваться информацией, согласовывать действия с коллегами и предоставлять пациентам необходимые данные. Однако использование email в медицинской практике требует особого внимания к безопасности и соблюдению этических норм, особенно когда речь идет о врачебной тайне. Электронная почта активно используется для передачи результатов обследований, назначений, консультаций и других медицинских данных. Например, врач может отправить коллеге результаты анализов пациента для получения второго мнения или направить заключение в другое медицинское учреждение для продолжения лечения. Однако такая передача информации требует особой осторожности:

- Конфиденциальность: нельзя указывать в письме полные ФИО пациента, диагнозы или другие персональные данные без шифрования.
- Идентификация: для защиты данных рекомендуется использовать уникальные идентификаторы пациента (например, номер истории болезни) вместо полных имен.

Электронная почта упрощает взаимодействие между врачами, особенно в случаях, когда требуется согласование диагноза или организация консилиума. Например, терапевт может отпра-

вить кардиологу данные пациента для уточнения тактики лечения. Однако важно помнить, что такая переписка должна быть защищена:

- Использование корпоративной почты с доменом медицинского учреждения.
- Шифрование писем при передаче конфиденциальной информации.

Несмотря на удобство, электронная почта имеет ряд ограничений в медицинской практике:

- Запрет на передачу незащищенных данных: Отправка персональных данных пациентов без шифрования может привести к утечке информации и нарушению врачебной тайны.
- Использование личной почты: Рабочая переписка должна вестись только через корпоративные email-адреса, чтобы минимизировать риски утечки данных.
- Ошибки при отправке: Случайная отправка письма не тому адресату может привести к серьезным последствиям, поэтому важно всегда проверять адреса получателей.

Электронная почта часто используется в связке с другими цифровыми инструментами, такими как Единая государственная информационная система здравоохранения (ЕГИСЗ) или электронная подпись. Например:

- Врач может отправить подписанное электронной подписью заключение через защищенный почтовый сервис.
- Автоматические уведомления из ЕГИСЗ (например, о новых назначениях или результатах анализов) могут поступать на корпоративную почту врача.

Для безопасного и эффективного использования электронной почты в медицинской практике рекомендуется:

- Использовать только корпоративные email-адреса.
- Шифровать письма при передаче конфиденциальной информации.
- Не указывать в письмах полные ФИО пациентов и диагнозы без необходимости.
- Регулярно проходить обучение по кибербезопасности.

Основой работы с электронной почтой является правильное оформление писем. Тема должна быть четкой и информативной, например, "Результаты МРТ пациента Х…, № истории болезни …». Это помогает адресату быстро понять содержание письма и избежать путаницы. В теле письма важно соблюдать профессиональный тон: избегать жаргона, быть лаконичным и точным. Подпись врача должна включать ФИО, должность и контактные данные, чтобы получатель мог легко связаться для уточнений.

Теперь понятно, что электронная почта — это не только удобство, но и риски. Передача персональных данных пациентов, таких как диагнозы, результаты анализов или назначения, требует особой осторожности. Ещё раз подчеркнем, что нельзя отправлять такие данные без шифрования, а также использовать личную почту для рабочих целей. Угрозы, такие как фишинг или взлом аккаунта, могут привести к утечке информации, что повлечет за собой не только профессиональные, но и юридические последствия.

Для минимизации рисков важно соблюдать меры безопасности: использовать двухфакторную аутентификацию, регулярно менять пароли и проверять адреса получателей перед отправкой. Шифрование писем с помощью технологий PGP или TLS также помогает защитить конфиденциальную информацию. Кроме того, врачам следует помнить о юридической ответственности за разглашение врачебной тайны, которая регулируется ст. 13 ФЗ-323 "Об основах охраны здоровья граждан".

Шифрование писем — это процесс преобразования текста сообщения в закодированную форму, чтобы защитить его от несанкционированного доступа. В медицинской практике, где конфиденциальность данных пациентов имеет критическое значение, шифрование становится необходимым инструментом для обеспечения безопасности. Две наиболее распространенные технологии для шифрования электронной почты — это PGP и TLS.

1. PGP (Pretty Good Privacy) — это технология шифрования, которая обеспечивает высокий уровень защиты данных. Она используется для шифрования как тела письма, так и вложенных файлов. PGP имеет открытый и закрытый ключи, используя их в системе. Открытый ключ доступен всем и используется для шифрования сообщений. Закрытый ключ известен только вла-

дельцу и используется для расшифровки. В процессе шифрования отправитель шифрует письмо с помощью открытого ключа получателя, получатель расшифровывает письмо своим закрытым ключом. PGP также позволяет подписывать письма, что гарантирует их подлинность и отсутствие изменений в процессе передачи.

Преимущества PGP: высокий уровень защиты, возможность шифрования вложений, поддержка цифровой подписи. Недостатки PGP: требует установки дополнительного программного обеспечения (например, Gpg4win, Kleopatra), необходимость обмена открытыми ключами между отправителем и получателем. PGP идеально подходит для передачи конфиденциальных данных, таких как результаты анализов, диагнозы или медицинские заключения. Например, врач может зашифровать результаты МРТ пациента и отправить их коллеге для консультации.

2. TLS (Transport Layer Security) — это протокол, который обеспечивает защиту данных при передаче между серверами. В отличие от PGP, TLS шифрует не само письмо, а канал связи, по которому оно передается. TLS обеспечивает:

- Защиту канала связи: когда письмо отправляется, TLS создает зашифрованное соединение между почтовым сервером отправителя и сервером получателя.
- Автоматическое шифрование: TLS работает на уровне серверов, поэтому пользователю не нужно предпринимать дополнительных действий.

Также для работы TLS почтовые серверы должны иметь действительные SSL/TLS-сертификаты безопасности. Преимущества TLS: простота использования: шифрование происходит автоматически. Она защищает данные во время передачи и широко поддерживается большинством почтовых сервисов (Gmail, Outlook, Яндекс.Почта и др.). Недостатки TLS: не защищает письмо после его доставки на сервер получателя и зависит от настроек почтовых серверов: если сервер получателя не поддерживает TLS, письмо будет передано без шифрования. TLS идеально подходит для повседневной переписки, например, для отправки уведомлений или организации встреч. Однако для пе-

редачи особо конфиденциальных данных рекомендуется дополнительно использовать PGP.

Таблица 1.

Достоинства и недостатки PGP и TLS в сравнении

Критерий	PGP	TLS
Что шифрует	Само письмо и вложения	Канал передачи данных
Уровень защиты	Высокий	Средний (зависит от серверов)
Простота использования	Требует настройки и обмена ключами	Работает автоматически
Идеальное применение	Передача конфиденциальных данных	Повседневная переписка

Теперь понятно, как использование технологий PGP и TLS позволяет врачам обеспечить безопасность электронной переписки и защитить конфиденциальные данные пациентов. PGP подходит для передачи особо важной информации, такой как медицинские заключения или результаты анализов, а TLS обеспечивает базовую защиту при повседневной переписке. Комбинирование этих технологий помогает соблюдать требования законодательства и сохранять доверие пациентов.

Регулярная смена паролей, двухфакторная аутентификация и проверка адресов получателей — это простые**,** но эффективные меры безопасности, которые помогают врачам минимизировать риски утечки данных и обеспечить конфиденциальность информации пациентов. Регулярная смена паролей — важная мера безопасности, которая помогает защитить учетные записи от взлома. Рекомендуется менять пароль каждые 3-6 месяцев, использовать сложные пароли, т.е. комбинации букв (заглавных и строчных), цифр и специальных символов, не использовать один и тот же пароль для разных сервисов. Следует помнить, что утечки данных происходят регулярно, и если пароль был скомпрометирован, его своевременная замена предотвратит доступ злоумышленников к вашей почте.

Двухфакторная аутентификация (2FA) добавляет дополнительный уровень защиты к вашей учетной записи. Она работает так: после ввода пароля требуется второй шаг подтверждения, например, код из SMS, приложения (Google Authenticator) или

биометрические данные (отпечаток пальца). Даже если пароль украден, злоумышленник не сможет войти без второго фактора, что повышает безопасность учетной записи на 90%. Необходимо использовать 2FA для всех важных сервисов, включая электронную почту и мессенджеры.

Кроме того, обязательно перед отправкой письма тщательно проверяйте адреса получателей, чтобы избежать случайной утечки данных. При этом: внимательно проверяйте адресную строку, особенно если используете автозаполнение; всегда убеждайтесь, что письмо отправляется именно тому адресату, кому оно предназначено; старайтесь не использовать групповую рассылку для конфиденциальной информации. Эти рекомендации крайне важны, поскольку ошибка в адресе может привести к отправке персональных данных пациента посторонним лицам, что нарушает врачебную тайну и может иметь юридические последствия.

Скажем несколько слов в отношении юридических аспектов, то есть об ответственности и условиях хранение переписки. В ст. 13 ФЗ-323 говорится об ответственности за разглашение врачебной тайны. Врачебная тайна — это конфиденциальная информация о состоянии здоровья пациента, диагнозах, методах лечения и других персональных данных. Ее разглашение без согласия пациента запрещено законом. Разглашением может считаться: передача данных третьим лицам (включая коллег, не участвующих в лечении), отправка информации по незащищенным каналам связи (например, через незашифрованную электронную почту), а также публикация данных в открытых источниках. При этом предусмотрены следующие виды ответственности:

- Дисциплинарная (выговор, увольнение).
- Административная (штрафы по ст. 13.14 КоАП РФ).
- Уголовная (в случае серьезных последствий — ст. 137 УК РФ).

Исключение составляет: передача данных по запросу правоохранительных органов или в рамках судебных разбирательств, угроза распространения инфекционных заболеваний, согласие пациента на разглашение.

Требования к хранению переписки (сроки, архивация) следующие: медицинские организации обязаны хранить переписку,

связанную с оказанием медицинской помощи, в соответствии с законодательством. Медицинская документация, включая электронную переписку, хранится не менее 5 лет (ст. 17 ФЗ-323), а в случае судебных разбирательств срок хранения может быть продлен. Переписка должна храниться в защищенном формате с ограниченным доступом. Рекомендуется использовать системы электронного документооборота (СЭД) для автоматической архивации и шифрования данных. Утрата или несанкционированное уничтожение медицинской документации может повлечь штрафы или дисциплинарные взыскания. Соблюдение этих требований помогает не только избежать юридических последствий, но и обеспечить доверие пациентов, что является основой профессиональной медицинской деятельности.

Единая государственная информационная система здравоохранения (ЕГИСЗ) активно использует электронную почту для уведомлений и автоматических рассылок, что упрощает взаимодействие врачей с системой. Например, врач получает на корпоративную почту уведомления о новых назначениях, поступивших в ЕГИСЗ (например, "Пациент Иванов Иван Иванович записан на прием к урологу"); или же происходит автоматическое оповещение о готовности результатов анализов или инструментальных исследований. Также могут осуществляться рассылки напоминаний пациентам о предстоящих приемах или необходимости пройти диспансеризацию, а также уведомления врачей о необходимости обновить данные в электронной медицинской карте (ЭМК) пациента. Мы получаем следующие преимущества: экономим наше время за счет автоматизации процессов, удобно получаем важную информацию напрямую на эл. почту.

Что важно знать об электронной подписи? ЭП — это инструмент, который позволяет врачам подписывать документы в электронном виде, придавая им юридическую силу. Вот пример её использования. Подписание вложенных документов:

- Врач формирует заключение или назначение, подписывает его электронной подписью и отправляет по электронной почте коллегам или пациентам. Например, терапевт отправляет подписанное направление на МРТ пациенту.
- Подписанные документы могут быть вложены в письмо в формате PDF или другом защищенном формате.

Другой пример. Взаимодействие с ЕГИСЗ:

- Врач подписывает электронной подписью данные, которые загружаются в ЕГИСЗ (например, результаты осмотра или диагноз).
- Подписанные документы могут быть отправлены через почту в случае технических сбоев в системе.

Преимущества очевидны: юридическая значимость документов, ускорение процессов согласования и передачи информации, удобство для пациентов, которые могут получать подписанные документы прямо на почту. В итоге использование электронной почты в связке с ЕГИСЗ и электронной подписью делает работу врачей более эффективной и безопасной, что позволяет быстро обмениваться информацией, соблюдать юридические требования и обеспечивать удобство для пациентов. Вот ещё несколько практических советов:

- Используйте корпоративные email-адреса с доменом медицинского учреждения.
- Не включайте в тело письма полные ФИО пациента и диагнозы без шифрования.
- Регулярно проходите тренинги по кибербезопасности (например, на портале "Госуслуги").

Итак, мы убедились в том, что электронная почта играет первую скрипку в интеграции с другими цифровыми системами, такими как ЕГИСЗ. То есть через email врачи могут получать уведомления о новых назначениях или отправлять подписанные электронной подписью документы. Это делает процесс взаимодействия более удобным и прозрачным. Поэтому можно уверенно говорить о том, что электронная почта — это мощный инструмент для врача, но его использование требует ответственности и внимания к деталям. Соблюдение правил безопасности, этикета и законодательства позволяет не только повысить эффективность работы, но и сохранить доверие пациентов, что является основой медицинской профессии.

Популярные мессенджеры в работе врача

Мессенджеры, такие как WhatsApp, Telegram и другие, стали неотъемлемой частью современной коммуникации. Их использование в медицинской практике имеет свои плюсы и минусы, которые важно учитывать для соблюдения врачебной тайны и обеспечения безопасности данных.

1. WhatsApp:
   - о Особенности: широко распространен, поддерживает текстовые сообщения, голосовые и видеозвонки, передачу файлов.
   - о Безопасность: использует сквозное шифрование, но данные резервируются в облаке (риск утечки).

2. Telegram:
   - о Особенности: поддерживает каналы, группы, передачу крупных файлов (до 2 ГБ).
   - о Безопасность: имеет секретные чаты с самоуничтожением сообщений, но обычные чаты шифруются не так надежно, как в WhatsApp.

3. Signal:
   - о Особенности: максимальная безопасность, открытый исходный код.
   - о Безопасность: считается золотым стандартом для обеспечения конфиденциальности переписки.

4. Роскомнадзор 13.12.2024 г. объявил о блокировке в России мессенджера Viber, поскольку Viber нарушает требования, которые необходимо выполнять в целях безопасности — чтобы мессенджер не использовали в террористических и экстремистских целях, а также для вербовки граждан.

Преимущества использования мессенджеров в работе врача следующие:

- оперативность, т. е. быстрый обмен информацией с коллегами (например, согласование диагноза или экстренный консилиум) и удобство для пациентов: можно быстро уточнить симптомы или получить рекомендации.

- удобство: возможность отправлять не только текст, но и фото, видео, документы (например, результаты анализов), а также голосовые сообщения экономят время.
- доступность: большинство мессенджеров работают на всех устройствах (смартфоны, планшеты, компьютеры), также бесплатное использование.

Здесь нельзя не упомянуть и ряде недостатков использования мессенджеров в работе врача.

- Риск утечки данных: далеко не все мессенджеры обеспечивают достаточный уровень шифрования; есть вероятность случайной отправки сообщения не тому адресату.
- Нарушение врачебной тайны: передача персональных данных пациентов через мессенджеры может нарушать законодательство (ст. 13 ФЗ-323); отсутствует контроль над хранением данных (например, резервные копии в облаке).
- Отсутствие интеграции с медицинскими системами: мессенджеры не связаны с ЕГИСЗ или электронными медицинскими картами, что усложняет документирование переписки.
- Этические вопросы: использование личных аккаунтов для профессиональной переписки может привести к смешению личной и рабочей жизни.

Можно предложить следующие рекомендации по безопасному использованию мессенджеров:

- Выбирайте безопасные мессенджеры: Signal или Telegram (с использованием секретных чатов).
- Не передавайте конфиденциальные данные: избегайте отправки полных ФИО пациентов, диагнозов или результатов анализов.
- Используйте рабочие аккаунты: создайте отдельный аккаунт для профессиональной переписки.
- Информируйте пациентов о рисках: получайте согласие на использование мессенджеров для общения.

Итак, мессенджеры представляют собой удобный инструмент для быстрой коммуникации, но их использование в медицинской практике требует осторожности. Соблюдение правил безопасности и этических норм поможет врачам избежать рисков и сохранить доверие пациентов.

Защита каналов связи

В медицинской практике защита каналов связи — это насущная необходимость, так как передача конфиденциальных данных пациентов требует соблюдения строгих норм безопасности. Рассмотрим основные методы защиты: шифрование данных, использование VPN и рекомендации по выбору безопасных каналов связи.

Шифрование представляет собой процесс преобразования информации в закодированную форму, чтобы только авторизованные пользователи могли ее прочитать.

Типы шифрования бывают:

- Сквозное шифрование: данные шифруются на устройстве отправителя и расшифровываются только на устройстве получателя (например, в WhatsApp, Signal).
- Шифрование при передаче: защищает данные только во время передачи между серверами (например, TLS для электронной почты).

Преимуществом шифрования является защита от перехвата данных и сохранение конфиденциальности даже при утечке информации. Мы рекомендуем использовать мессенджеры и почтовые сервисы с поддержкой сквозного шифрования (Signal, ProtonMail), а для электронной почты следует применять PGP-шифрование для защиты тела письма и вложений.

VPN (Virtual Private Network) — это технология, которая создает защищенное соединение между устройством пользователя и интернетом, маскируя IP-адрес и шифруя весь трафик. В отношении преимуществ VPN необходимо отметить: защиту данных при использовании общедоступных Wi-Fi сетей (например, в больнице или кафе), обход географических ограничений (полезно для доступа к зарубежным медицинским ресурсам) и анонимность в сети. Мы рекомендуем выбирать надежные VPN-сервисы с прозрачной политикой конфиденциальности (например, NordVPN, ExpressVPN), а также использовать VPN при работе с конфиденциальными данными вне защищенных сетей.

Кроме того, по вопросу выбора безопасных каналов связи необходимо заметить, что для повседневной переписки лучше использовать мессенджеры с поддержкой сквозного шифрования (Signal, Telegram в режиме секретных чатов), избегая передачи

конфиденциальных данных через обычные SMS или незащищенные приложения.

Для передачи медицинских данных надо использовать специализированные платформы, соответствующие требованиям законодательства (например, защищенные порталы для телемедицины), а также электронную почту с шифрованием PGP и TLS для защиты канала передачи. В ходе удаленной работы следует осуществлять подключение к корпоративным сетям через VPN и использовать двухфакторную аутентификацию для доступа к рабочим ресурсам.

Общие рекомендации таковы: регулярно обновлять программное обеспечение для защиты от уязвимостей; проводить обучение сотрудников основам кибербезопасности (например, как распознать фишинг); обязательно использовать антивирусные программы и брандмауэры для дополнительной защиты.

Подводя итог, ещё раз подчеркнём, что защита каналов связи является наиважнейшим аспектом организации врачебной деятельности в цифровую эпоху. Шифрование данных, использование VPN и выбор безопасных каналов связи помогают минимизировать риски утечки информации и строго следовать требованиям законодательства РФ. Соблюдение этих мер не только защищает данные пациентов, но и упрочивает доверие населения к конкретному медицинскому учреждению.

ГЛАВА 2. ЭЛЕКТРОННАЯ ПОДПИСЬ И ЕЕ ПРИМЕНЕНИЕ

Электронная подпись (ЭП) — это технология, позволяющая подтверждать подлинность электронных документов и обеспечивать их юридическую значимость. В медицине электронная подпись играет важную роль, так как способствует повышению безопасности, конфиденциальности и эффективности обработки медицинских данных. Рассмотрим основные аспекты применения электронной подписи в медицине.

Электронная подпись является аналогом собственноручной подписи, но в цифровом формате. Она создается с использованием криптографических методов и позволяет: удостоверить личность подписанта, обеспечить целостность документа (исключить возможность внесения изменений после подписания), защитить данные от несанкционированного доступа.

ЭП бывает 3 видов:

1) Простая — подтверждает факт подписания, но не гарантирует юридическую значимость.
2) Усиленная неквалифицированная — обеспечивает более высокий уровень защиты и может использоваться для внутреннего документооборота.
3) Усиленная квалифицированная — имеет максимальную юридическую силу и требует сертифицированных средств криптозащиты.

В медицинской сфере электронная подпись используется для решения следующих задач:

Электронный документооборот

- Медицинские карты и рецепты: ЭП позволяет врачам подписывать электронные медицинские карты, рецепты и направления, что ускоряет процесс обработки данных и снижает вероятность ошибок.
- Отчеты и справки: Лабораторные результаты, заключения и другие медицинские документы могут быть подписаны электронной подписью, что делает их юридически значимыми.

Дистанционные консультации и телемедицина

- Подписание консультаций: Врачи могут подписывать результаты дистанционных консультаций, что особенно важно в условиях пандемий или для пациентов из удаленных регионов.
- Назначение лечения: ЭП позволяет врачам назначать лечение и выписывать рецепты онлайн, что упрощает доступ пациентов к медицинской помощи.

Защита персональных данных

- Конфиденциальность: ЭП обеспечивает защиту персональных данных пациентов, что соответствует требованиям законодательства (например, GDPR в Европе или ФЗ-152 в России).
- Контроль доступа: только авторизованные лица с электронной подписью могут получать доступ к медицинским данным.

Клинические исследования

- Подписание протоколов: в клинических исследованиях ЭП используется для подписания протоколов, отчетов и других документов, что обеспечивает их достоверность и юридическую силу.
- Сбор данных: ЭП позволяет подтверждать подлинность данных, собранных в ходе исследований.

Взаимодействие с государственными органами

- Отчетность: медицинские учреждения могут сдавать отчеты в контролирующие органы в электронном виде, подписанные ЭП.
- Лицензирование и аккредитация: ЭП используется для подачи заявок на получение лицензий и аккредитации.

Электронная подпись имеет неоспоримые преимущества перед обычной подписью, поскольку она обеспечивает:

- Сокращение времени обработки документов: Устранение необходимости в бумажных носителях ускоряет процессы.
- Повышение безопасности данных: Криптографическая защита снижает риск утечки информации.
- Удобство для пациентов: Пациенты могут получать медицинские услуги и документы онлайн.

- Снижение затрат: Уменьшение расходов на бумагу, печать и доставку документов.

Коснёмся также правовых аспектов применения ЭП в сфере здравоохранения. В большинстве стран её использование в медицине регулируется законодательством. Например, в России это Федеральный закон №63-ФЗ "Об электронной подписи" и Федеральный закон №323-ФЗ "Об основах охраны здоровья граждан". В Европейских странах действует Регламент eIDAS, который устанавливает стандарты для электронных подписей.

Приведем основные направления использования ЭП в медицине:

- Электронные рецепты: врач выписывает рецепт, подписывает его ЭП, и пациент может получить лекарство в аптеке, предъявив электронный документ.
- Электронные больничные листы: работодатель получает больничный лист, подписанный ЭП, что исключает возможность подделки.
- Телемедицинские платформы: пациент консультируется с врачом онлайн, а результаты консультации подписываются ЭП.

По всей видимости, здесь будет не лишним упомянуть о некоторых животрепещущих проблемах и вызовах, касающихся использования ЭП. К ним относятся:

- Техническая сложность: внедрение ЭП требует наличия инфраструктуры и обучения персонала.
- Стоимость: получение квалифицированной электронной подписи и средств криптозащиты может быть затратным.
- Недостаточная осведомленность: не все медицинские работники и пациенты знают о возможностях ЭП.

Дадим пошаговую инструкцию того, как получить и настроить электронную подпись, поскольку ЭП является сложным инструментом, который требует грамотного и бережного обращения, а также правильной настройки.

Шаг 1: Определите тип электронной подписи

1. Простая ЭП — используется для внутреннего документооборота и не требует специальных средств криптозащиты.

2. Усиленная неквалифицированная ЭП — подходит для большинства задач, включая подписание документов внутри организации.
3. Усиленная квалифицированная ЭП — имеет максимальную юридическую силу и используется для взаимодействия с государственными органами, налоговой службой и другими организациями.

Для медицинской сферы чаще всего требуется усиленная квалифицированная электронная подпись.

Шаг 2: Выберите удостоверяющий центр (УЦ)

Удостоверяющий центр — это организация, которая выдает электронные подписи. Убедитесь, что у УЦ есть аккредитация. В России это центры, аккредитованы Минцифры.

Шаг 3: Подготовьте документы

Для получения ЭП потребуются: паспорт, ИНН (или другой идентификационный номер), заявление на получение ЭП (оформляется в УЦ), а для юридических лиц ещё нужны дополнительные документы (выписка из ЕГРЮЛ, доверенность и т.д.).

Шаг 4: Получите электронную подпись

Для этого подайте заявление в удостоверяющий центр, оплатите услугу (стоимость зависит от типа ЭП и срока действия) и, наконец, получите комплект, в который входят сертификат электронной подписи (файл или токен), программное обеспечение для работы с ЭП (например, КриптоПро), а также инструкция по установке и использованию.

Шаг 5: Установите и настройте ЭП

Установите ПО для работы с ЭП. В России такой программой является КриптоПро CSP или другие крипто провайдеры. Далее настройте сертификат в соответствии с инструкцией УЦ, подключив токен или загрузив сертификат. Если используется токен (USB-носитель), то подключите его к компьютеру. Если сертификат представлен в виде файла, то установите его через интерфейс криптопровайдера. В завершении проверьте работоспособность, попробовав подписать тестовый документ и убедившись, что подпись проходит проверку.

Шаг 6: Используйте ЭП

Подписывайте документы через поддерживаемые программы (например, Microsoft Word, Adobe Acrobat, специализированные медицинские системы). Каждый раз убеждаясь, что документы сохраняют юридическую значимость после подписания.

Обратите внимание на р**екомендации по хранению и защите электронной подписи**

1. Хранение сертификата ЭП

- Токены (USB-носители): Используйте защищенные токены (например, Рутокен или eToken). Они защищены от копирования и взлома.
- Файлы: Если сертификат хранится в виде файла, сохраните его на защищенном носителе (например, зашифрованная флешка или жесткий диск).
- Облачное хранилище: Некоторые УЦ предлагают облачное хранение сертификатов, но это менее безопасный вариант.

2. Защита паролей

Установите сложный пароль для доступа к сертификату ЭП. Не передавайте пароль третьим лицам. Регулярно меняйте пароль.

3. Защита от вирусов и взлома

Установите антивирусное ПО на устройство, где используется ЭП. Не используйте ЭП на общедоступных или ненадежных компьютерах. Регулярно обновляйте крипто провайдер (например, КриптоПро).

4. Резервное копирование

Обязательно создайте резервную копию сертификата и храните ее в безопасном месте, а также убедитесь, что резервная копия также защищена паролем.

5. Срок действия сертификата

Непременно следите за сроком действия сертификата ЭП. Он обычно составляет 1 год, поэтому заблаговременно продлевайте сертификат в удостоверяющем центре.

6. Уничтожение ЭП

Если ЭП больше не нужна, удалите сертификат и уничтожьте носитель (например, токен), убедившись, что данные невозможно восстановить.

Как теперь очевидно, получение и настройка электронной подписи представляет собой достаточно сложный процесс, который требует внимания к деталям. Следуя инструкции и рекомендациям по хранению и защите, вы сможете обеспечить безопасное и эффективное использование ЭП в медицинской организации. Это не только упростит документооборот, но и защитит конфиденциальные данные пациентов.

Логично сделать общий вывод, что на сегодняшний день электронная подпись постепенно становится неотъемлемым практическим элементом отечественной медицины, обеспечивая безопасность, удобство и юридическую значимость электронных документов. Ее повсеместное внедрение способствует цифровизации здравоохранения России, улучшению качества медицинских услуг и защите данных пациентов. Однако для более широкого и успешного использования ЭП в будущем потребуется решить ряд технических, организационных и правовых вопросов, о которых мы постарались упомянуть на страницах настоящего методического пособия.

ГЛАВА 3. ЕДИНАЯ ГОСУДАРСТВЕННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ЗДРАВООХРАНЕНИЯ

Единая государственная информационная система в сфере здравоохранения (ЕГИСЗ) — это масштабная цифровая платформа, созданная для интеграции и управления данными в системе здравоохранения России. Она была разработана в рамках программы цифровизации здравоохранения и начала активно внедряться с 2017 года.

Основные цели ЕГИСЗ:

1. Централизация данных: Сбор и хранение информации о пациентах, медицинских учреждениях, врачах, лекарственных препаратах и медицинских услугах в единой системе.
2. Упрощение документооборота: Переход на электронные медицинские карты, рецепты, направления и другие документы.
3. Повышение качества медицинской помощи: Быстрый доступ к данным пациента, что позволяет врачам принимать более обоснованные решения.
4. Контроль и аналитика: Мониторинг работы медицинских учреждений, анализ заболеваемости и эффективности лечения.
5. Интеграция с другими системами: Взаимодействие с системой обязательного медицинского страхования (ОМС), аптеками, лабораториями и другими участниками системы здравоохранения.

К основным компонентам ЕГИСЗ относятся:

- Электронная медицинская карта (ЭМК). Она содержит всю информацию о здоровье пациента: диагнозы, назначения, результаты анализов, историю обращений и т. д. Кроме того, она доступна врачам из разных медицинских учреждений (с согласия пациента).
- Электронные рецепты, если врач выписывает рецепт в электронном виде, то пациент может получить лекарство в аптеке по этому рецепту.

- Регистр медицинских работников, который содержит данные о врачах, их квалификации, сертификатах и лицензиях.
- Регистр медицинских организаций с информацией о больницах, поликлиниках, лабораториях и других учреждениях.
- Система мониторинга лекарственных препаратов, которая осуществляет контроль за оборотом лекарств, включая льготные препараты.

Врач, безусловно, является одним из ключевых пользователей ЕГИСЗ. Его роль в системе включает следующие аспекты:

1. Ведение электронной медицинской карты (ЭМК)

Врач заполняет ЭМК пациента, внося данные о диагнозах, назначениях, результатах обследований и лечении, что позволяет другим специалистам быстро получить доступ к информации о пациенте, и что особенно важно при оказании экстренной помощи или при проведении консультаций.

2. Выписка электронных рецептов

Врач выписывает рецепты в электронном виде через систему ЕГИСЗ, а пациент может получить лекарство в любой аптеке, подключенной к системе.

3. Назначение диагностических процедур

Врач оформляет направления на анализы, инструментальные исследования и другие процедуры в электронном виде, а результаты автоматически загружаются в ЭМК пациента.

4. Взаимодействие с другими специалистами

Врач может запрашивать консультации у коллег, делиться данными пациента и получать обратную связь через систему.

5. Контроль качества лечения

Врач может использовать данные ЕГИСЗ для анализа эффективности назначенного лечения и корректировки плана при необходимости.

6. Отчетность и статистика

Врач участвует в формировании отчетов для вышестоящих органов (например, данные о заболеваемости, выполнении нормативов и т.д.), что, несомненно, помогает улучшить качество медицинской помощи на уровне региона и страны в целом.

7. Работа с системой ОМС

Врач вносит данные о предоставленных услугах, что необходимо для расчетов с фондом обязательного медицинского страхования.

Для врачей ЕГИСЗ обладает следующими преимуществами:

- Упрощение работы: Снижение бумажной нагрузки, автоматизация рутинных процессов.
- Доступ к данным: Возможность быстро получить информацию о пациенте, даже если он ранее обращался в другое учреждение.
- Повышение качества лечения: Использование актуальных данных для принятия решений.
- Юридическая защита: Все действия врача фиксируются в системе, что помогает в спорных ситуациях.

Вместе с тем в работе с ЕГИСЗ медработники сталкиваются с рядом проблем, среди которых можно выделить:

- Технические сложности: не все врачи легко осваивают новые технологии.
- Загруженность: внесение данных в систему отнимает у врача дополнительное время.
- Защита данных: необходимость строгого соблюдения конфиденциальности информации о пациентах.
- Зависимость от интернета: работоспособность системы прямо зависит от стабильного подключения к сети.

По этим причинам работа с Единой государственной информационной системой в сфере здравоохранения требует внимательности и жесткого соблюдения определенных правил. Надо признать, что даже опытные пользователи могут допускать ошибки, которые могут привести к проблемам в работе системы, потере данных или нарушению конфиденциальности. Рассмотрим типичные ошибки при работе с ЕГИСЗ и способы их устранения.

1. Ошибки при вводе данных

Типичные ошибки: Неполное заполнение электронной медицинской карты (ЭМК); Ошибки в написании диагнозов, назначений или данных пациента (например, неправильная дата рождения или ФИО); Некорректное оформление электронных рецептов или направлений. Способы устранения: Внимательным

образом проверяйте вводимые данные перед сохранением; Используйте справочники и классификаторы, встроенные в систему (например, МКБ-10 для диагнозов); Нужно регулярное обучение персонала по работе с ЕГИСЗ.

2. Нарушение сроков внесения данных

Типичные ошибки: Задержка в заполнении ЭМК или оформлении рецептов; Несвоевременное внесение данных о проведенных процедурах или лечении. Способы устранения: Внедрите регламент работы с системой, требующий оперативного внесения данных; Назначьте ответственных за контроль сроков заполнения данных; Используйте напоминания или уведомления в системе.

3. Проблемы с доступом к системе

Типичные ошибки: Потеря логина или пароля; Попытка войти в систему с неподдерживаемого устройства или браузера; Неправильная настройка рабочего места (например, отсутствие необходимого ПО). Способы устранения: Храните учетные данные в надежном месте (например, в зашифрованном файле или менеджере паролей); Используйте только поддерживаемые браузеры и устройства (обычно это указано в инструкции к системе); Обратитесь в техническую поддержку для настройки рабочего места.

4. Нарушение конфиденциальности данных

Типичные ошибки: Передача учетных данных (логина и пароля) третьим лицам; Работа с системой на общедоступных компьютерах без защиты; Неправильная настройка прав доступа для сотрудников. Способы устранения: Никогда не передавайте свои учетные данные другим лицам; Используйте двухфакторную аутентификацию, если она доступна; Работайте с системой только на защищенных устройствах с установленным антивирусным ПО; Настройте права доступа в соответствии с должностными обязанностями сотрудников.

5. Ошибки при работе с электронными рецептами

Типичные ошибки: Неправильное оформление рецепта (например, ошибка в дозировке или названии препарата); Отсутствие подписи электронной подписью (ЭП); Несвоевременная отмена или изменение рецепта. Способы устранения: Внимательно проверяйте данные перед отправкой рецепта; Убедитесь,

что рецепт подписан электронной подписью; Обучите персонал правилам оформления рецептов в ЕГИСЗ.

6. Проблемы с интеграцией ЕГИСЗ и других систем

Типичные ошибки: Данные из ЕГИСЗ не синхронизируются с другими системами (например, с лабораторной информационной системой или системой ОМС); Ошибки при передаче данных между медицинскими учреждениями. Способы устранения: Проверьте настройки интеграции и убедитесь, что все системы совместимы; Обратитесь в техническую поддержку ЕГИСЗ для устранения неполадок; Регулярно обновляйте программное обеспечение.

7. Неправильное использование электронной подписи (ЭП)

Типичные ошибки: Подписание документов без проверки их содержания; Использование ЭП на ненадежных устройствах; Потеря токена или утечка данных сертификата. Способы устранения: Всегда проверяйте документы перед подписанием; Храните токен или сертификат ЭП в безопасном месте; Установите пароль на доступ к сертификату и регулярно его меняйте.

8. Игнорирование обновлений системы

Типичные ошибки: Работа с устаревшей версией системы; Игнорирование уведомлений о необходимости обновления. Способы устранения: Регулярно проверяйте наличие обновлений и устанавливайте их; Назначьте ответственного за контроль обновлений в медицинском учреждении.

9. Неправильное обращение с технической поддержкой

Типичные ошибки: Попытка самостоятельно устранить сложные технические проблемы; Непредоставление достаточной информации при обращении в поддержку. Способы устранения: При возникновении сложных проблем сразу обращайтесь в техническую поддержку ЕГИСЗ. Подготовьте подробное описание проблемы, скриншоты и логи (если возможно).

10. Недостаточное обучение персонала

Типичные ошибки: Сотрудники не знают, как правильно работать с системой; Отсутствие регулярного обучения новым функциям ЕГИСЗ. Способы устранения: Организуйте обучение для всех сотрудников, работающих с ЕГИСЗ; Проводите регулярные тренинги и обновляйте инструкции.

В общем при работе с ЕГИСЗ мы настоятельно рекомендуем учитывать все вышеперечисленные правила и нюансы. В частности, как уже упоминалось нужно освоить систему, пройдя обучение, предоставляемое медицинским учреждением или разработчиками ЕГИСЗ. Важно строго соблюдать регламент, внося все необходимые данные своевременно и в полном объеме. Необходимо заботиться о защите данных, не передавать свои учетные данные (логин и пароль) третьим лицам. Следует максимально использовать все возможности системы, активно применяя функции ЕГИСЗ для улучшения качества и повышения доступности медицинской помощи.

Итак, ЕГИСЗ есть надежный и важный инструмент для цифровизации здравоохранения, который помогает врачам работать более эффективно и предоставлять пациентам качественную медицинскую помощь. Роль врача в системе заключается не только в лечении пациентов, но и в активном использовании цифровых технологий для улучшения процессов диагностики, лечения и отчетности.

ГЛАВА 4. ПОРТАЛ ГОСУДАРСТВЕННЫХ УСЛУГ И ЕСИА

Портал госуслуг (gosuslugi.ru) — это единая платформа, предоставляющая гражданам и организациям доступ к государственным и муниципальным услугам в электронном виде. Для медицинских работников в России портал госуслуг предлагает множество полезных функций, которые упрощают профессиональную деятельность, взаимодействие с государственными органами и доступ к важной информации. Рассмотрим основные возможности портала для медицинских работников.

1. Получение и продление лицензий и сертификатов

Медицинские работники могут: подать заявление на получение или продление сертификата специалиста; оформить лицензию на медицинскую деятельность (для ИП или организаций); отслеживать статус заявлений и получать уведомления о готовности документов.

2. Доступ к данным ЕГИСЗ (Единой государственной информационной системы в сфере здравоохранения). Через портал госуслуг медицинские работники могут: получать доступ к электронным медицинским картам (ЭМК) пациентов (с их согласия); оформлять электронные рецепты и направления на диагностику; просматривать результаты анализов и обследований.

3. Взаимодействие с ФОМС (Фондом обязательного медицинского страхования). Медицинские работники могут: проверять статус регистрации пациента в системе ОМС; получать информацию о талонах на прием и оказанных медицинских услугах; контролировать финансовые расчеты за оказанные услуги.

4. Участие в программе «Земский доктор» и «Земский фельдшер». Через портал госуслуг можно: подать заявление на участие в программе "Земский доктор" или "Земский фельдшер"; получить информацию о выплатах и условиях программы; отслеживать статус заявки.

5. Повышение квалификации и аккредитация. Медицинские работники могут: зарегистрироваться на курсы повышения квалификации; подать заявление на аккредитацию или переаккредитацию; получить доступ к образовательным ресурсам и тестам.

6. Налоговые и пенсионные услуги. Через портал госуслуг можно: проверить налоговые начисления и оплатить налоги; получить информацию о пенсионных отчислениях; оформить льготы или вычеты (например, за обучение или лечение).

7. Участие в государственных программах и грантах. Медицинские работники могут: подать заявку на участие в государственных программах поддержки здравоохранения; получить информацию о грантах для научных исследований или внедрения инноваций.

8. Получение справок и выписок. Через портал госуслуг можно: заказать справку об отсутствии судимости (например, для трудоустройства); получить выписку из трудовой книжки; оформить справку о доходах (например, для кредита).

9. Участие в электронных аукционах и закупках. Для медицинских организаций и ИП есть возможность участвовать в электронных аукционах на поставку медицинского оборудования или лекарств, а также организован доступ к реестру закупок и государственным контрактам.

10. Получение информации о новых нормативных актах. Медицинские работники могут: получать уведомления о новых законах и нормативных актах в сфере здравоохранения; знакомиться с изменениями в трудовом законодательстве.

11. Упрощение отчетности. Через портал госуслуг можно: сдавать отчеты в контролирующие органы (например, в Росздравнадзор); получать доступ к статистическим данным и аналитическим отчетам.

12. Личный кабинет медицинского работника. Портал госуслуг предоставляет личный кабинет, где можно: управлять своими данными (например, обновить контактную информацию); получать уведомления о новых услугах и возможностях;

хранить электронные документы (например, сертификаты, лицензии).

13. Участие в опросах и обратная связь. Медицинские работники могут: участвовать в опросах и анкетировании, проводимых Минздравом или другими органами; оставлять обратную связь по улучшению работы системы здравоохранения.

14. Доступ к справочным материалам. Через портал госуслуг можно: получить доступ к справочникам (например, МКБ-10) и ознакомиться с рекомендациями по лечению и диагностике.

15. Упрощение трудоустройства. Медицинские работники могут: разместить свое резюме на портале; получить доступ к вакансиям в медицинских учреждениях.

Если Вы решили начать использовать портал госуслуг, то ваш порядок действий должен быть следующим:

- Зарегистрируйтесь на портале gosuslugi.ru.
- Подтвердите свою учетную запись (через МФЦ, онлайн-банкинг или почту).
- Заполните профиль, указав свои профессиональные данные (например, номер сертификата специалиста).
- Начните пользоваться доступными услугами.

Портал госуслуг имеет для медицинских работников ряд преимуществ:

- Удобство: доступ к услугам в любое время и из любого места.
- Экономия времени: отсутствие необходимости посещать государственные органы лично.
- Прозрачность: возможность отслеживать статус заявлений и документов.
- Безопасность: защита персональных данных с использованием современных технологий.

Итак, можно констатировать, что портал госуслуг предоставляет медицинским работникам в России широкий спектр возможностей для упрощения профессиональной деятельности, взаимодействия с государственными органами и доступа к важной информации. Использование портала помогает сэкономить время, снизить бюрократическую нагрузку и повысить эффективность работы в отрасли здравоохранения.

ЕСИА (Единая система идентификации и аутентификации) — это централизованная система, разработанная для упрощения доступа граждан и организаций к государственным и муниципальным услугам в электронном виде. ЕСИА позволяет пользователям получать доступ к различным информационным системам и сервисам с использованием единой учетной записи.

ЕСИА обеспечивает:

- Упрощение доступа к услугам, поскольку ЕСИА позволяет использовать одну учетную запись для доступа к множеству государственных и коммерческих сервисов (например, портал госуслуг, налоговые услуги, медицинские системы).
- Безопасность, так как ЕСИА обеспечивает защиту персональных данных за счет использования современных технологий шифрования и двухфакторной аутентификации.
- Снижение бюрократической нагрузки на население за счет упрощения процесса идентификации пользователей и устранения необходимости многократной регистрации в разных системах.
- Системную интеграцию путем объединения различных информационных систем, что позволяет обмениваться данными между ними (например, между ЕГИСЗ и порталом госуслуг).

Медицинские работники и пациенты могут использовать ЕСИА для доступа к медицинским информационным системам, таким как ЕГИСЗ (Единая государственная информационная система в сфере здравоохранения) или электронные медицинские карты (ЭМК). Рассмотрим пошагово, как это сделать.

Шаг 1: Регистрация в ЕСИА

- Перейдите на портал gosuslugi.ru.
- Нажмите кнопку "Зарегистрироваться".
- Заполните необходимые данные: ФИО, номер телефона или адрес электронной почты, паспортные данные и СНИЛС (для подтвержденной учетной записи).
- Подтвердите свою учетную запись либо через МФЦ (личное посещение), либо с помощью онлайн-банкинга (например, Сбербанк, Тинькофф), либо через почту России (код подтверждения придет заказным письмом).

Шаг 2: Получение доступа к медицинским системам

- Для пациентов: Авторизуйтесь на портале госуслуг; Перейдите в раздел "Здоровье"; Получите доступ к своей электронной медицинской карте (ЭМК), результатам анализов, записи к врачу и другим услугам.
- Для медицинских работников: Авторизуйтесь на портале госуслуг или в специализированной медицинской системе (например, ЕГИСЗ); Используйте свою учетную запись ЕСИА для входа в систему.

Шаг 3: Работа с медицинскими системами

- Для пациентов: Просматривайте свои медицинские данные (диагнозы, назначения, результаты анализов); Записывайтесь на прием к врачу; Получайте электронные рецепты; Оформляйте больничные листы.
- Для медицинских работников: Ведите электронные медицинские карты (ЭМК) пациентов; Выписывайте электронные рецепты; Оформляйте направления на диагностику; Получайте доступ к данным пациентов из других медицинских учреждений (с их согласия).

К преимуществам использования ЕСИА в медицине можно отнести:

- Удобство: Единый вход в различные медицинские системы.
- Экономию времени: Упрощение доступа к данным и услугам.
- Безопасность: Защита персональных данных пациентов и медицинских работников.
- Интеграцию: Возможность обмена данными между системами (например, ЕГИСЗ, портал госуслуг, ФОМС).

Продемонстрируем варианты использования ЕСИА в медицине на конкретных примерах:

- Электронная медицинская карта (ЭМК): Пациент может просматривать свои данные, а врач — вносить изменения и дополнения.
- Электронные рецепты: Врач выписывает рецепт через систему, а пациент получает лекарство в аптеке по этому рецепту.
- Запись на прием: Пациент записывается к врачу через портал госуслуг, используя учетную запись ЕСИА.

- Доступ к результатам анализов: Пациент может просматривать результаты анализов онлайн, а врач — использовать их для постановки диагноза.

В качестве рекомендаций по использованию ЕСИА советуем соблюдать следующие правила:

- Всячески защищать свои данные, т.е. не передавать логин и пароль от учетной записи третьим лицам и использовать только сложные пароли и двухфакторную аутентификацию.
- Регулярно обновлять информацию, убеждаясь, что ваши данные в ЕСИА актуальны (например, контактная информация).
- При возникновении проблем с доступом или использованием ЕСИА обращаться в техническую поддержку портала госуслуг.

Подчеркнём, что ЕСИА является ключевым инструментом для доступа к государственным и медицинским услугам в электронном виде, который упрощает работу медицинских работников и повышает удобство для пациентов, обеспечивая безопасный и быстрый доступ к данным. Использование ЕСИА в медицине способствует углублению процесса цифровизации здравоохранения, улучшению качества медицинских услуг и снижению бюрократической нагрузки на врачей.

ГЛАВА 5. ЦИФРОВАЯ ЭТИКА В ЗДРАВООХРАНЕНИИ И ЗАЩИТА ДАННЫХ

Цифровая трансформация медицины актуализировала этические вопросы, которые стали ключевыми и определяют развитие сквозных технологий в этой сфере: большие данные, искусственный интеллект, автоматизацию и робототехнику. К ним можно отнести: права пациентов в цифровом здравоохранении, ответственное поведение медицинских работников в цифровом здравоохранении, управление данными здравоохранения и равенство в цифровом здравоохранении. Некоторые исследователи выделяют 8 основных проблем, связанных с цифровизацией: 1) большие данные («цифровые двойники» и фальсификации); 2) метаморфозы отношений практикующего врача и пациента; 3) цифровая грамотность пациентов; 4) принятие ответственности в комплексных системах; 5) сопутствующие изменения в палитре медицинских специальностей; 6) рост затрат и риски чрезмерного лечения; 7) цифровой след; 8) место клинических данных в лечении и их конфиденциальность.

Совершенно очевидно, что эти технологии существенно изменили диагностику, систему профилактики заболеваний и лечение, взаимоотношения врача и пациента. Вместе с тем мы видим, что на практике, например, применение больших данных при обучении искусственного интеллекта может приводить к манипуляции и дискриминации, нарушая права и свободы человека. В то же время, ограничивая процесс цифровизации медицины, мы замедляем прогресс в этой сфере и снижаем конкурентоспособность отечественного здравоохранения. Обращаясь к истории медицины, мы понимаем, что сбор информации и сбор анамнеза входят в золотой стандарт лечения. Но только цифровая трансформация изменила объем и расширила возможности сбора, хранения и анализа данных. Совершенно очевидно, что сегодня данные, касающиеся здоровья человека и его физического состояния могут собираться разными способами и не всегда могут быть связаны с оказанием медицинской помощи. Так к источникам данных в медицине в широком смысле относятся:

– электронные медицинские карты;
– мобильные приложения для здравоохранения, в формате информационных баз данных;
– датчики и устройства мониторинга;
– данные лабораторных исследований, рентгеновские снимки;
– данные портала госуслуг о вакцинации и ПЦРтестах;
– данные, полученные в ходе клинических исследований с участием групп пациентов;
– данные о покупке лекарств и других средств медицинской помощи пациентами;
– данные соцсетей, поисковых запросов и т. д.

Как отмечают специалисты по искусственному интеллекту, для того чтобы его максимально использовать в профилактике и лечении заболеваний нужно больше данных, причём не только медицинских, но и социальных. И тут возникает этическая проблема, связанная с защитой персональной информации, которая не является только медицинской. Эти данные (информация) содержатся на различных платформах и хранилищах, не всегда друг с другом совместимых, регулируемых законодательными базами. Для того чтобы их использовать в целях сохранения здоровья и лечения человека требуются: качественные и верифицированные данные, совместимость систем хранения этих данных, их стандартизация и унификация и конечно, выработка этических норм и правил их использования.

Особое место в соблюдении этических норм в условиях цифровизации медицины играют общие принципы биоэтики, касающиеся автономии личности, конфиденциальности, соотношения риска и пользы, вопросы равенства и доступности. Наиболее полно они отражены в документе «Всеобщая декларация о биоэтике и правах человека» (ЮНЕСКО, 2005). Ещё один мега актуальный вопрос современности вызывает беспокойство, связанное с применением информационных технологий: каковы границы цифрового контроля поведения человека? Он затрагивает поведение человека и его отношение к своему здоровью — речь идет не о прямой связи цифровой медицины и этики, а о том, что цифровая технология опосредованно оказывается определенной мерой контроля этичности поведения человека. Об этом нужно задуматься, когда речь идёт о здоровье индивида и общества в условиях чрезвычайных ситуаций, например, как в

случае пандемии COVID-19. В международной повестке защиты прав человека это нашло отражение в формировании новых подходов к соблюдению этических принципов в этих условиях. Так, в Великобритании Совет Наффилда, считающийся главным мировым исследовательским центром по биоэтике, сформулировано мнение о необходимости следовать разным этическим принципам в зависимости от ситуации. Другими словами, нет единого правила. Каждый раз создается небольшая группа, принимающая решения масштаба «жизни и смерти» и разрабатывающая некий «этический компас» для конкретной ситуации.

Важно и то, что этические нормы должны соблюдаться не только работниками медицины и здравоохранения, но и разработчиками программных продуктов, связанных с использованием искусственного интеллекта, операторами и иными лицами, кому приватная информация окажется известной в силу исполнения профессиональных обязанностей (речь идет о профилактике нарушений врачебной тайны, права на защиту частной жизни, гарантии защиты персональных данных). Одной из проблем для тех, кто занимается проектированием, разработкой и внедрением цифровых технологий и приложений в области здравоохранения, будет определение того, что представляет собой этическую проблему и каких этических стандартов следует придерживаться.

Существует множество регламентов и руководящих принципов, направленных на борьбу с влиянием цифровых технологий на население. Инженеры по разработке и адаптации программных продуктов для медицины должны придерживаться соответствующих кодексов этики для выполнения важных требований к программному обеспечению, связанных с инженерной этикой. В свою очередь, разработка и внедрение цифровых технологий и приложений в области здравоохранения будет определять, каким этическим стандартам необходимо следовать. Таким образом, назрела необходимость создания соответствующих профессиональных поведенческих кодексов для представителей этих новых специальностей, которые объединят в себе этические требования к программному обеспечению, положения инженерной этики и этические стандарты, принятые в медицинской практике. Вместе с тем, разработка современных этических стандартов цифровой трансформации медицины не должна носить запретительный характер, она должна быть регулирующей

и предоставлять возможность широкого развития и внедрения информационных сквозных технологий для повышения качества жизни населения.

Согласно действующему российскому законодательству, к персональным данным относится любая информация, которая прямо или косвенно относится к физическому лицу — субъекту персональных данных, т. е. к этой категории можно отнести достаточно большой объем различных сведений. Важно отметить, что проводимая на основе использования персональных данных идентификация личности пациента, а также принадлежности к нему сведений, полученных в ходе обследования, и назначенного лечения — ключевой аспект безопасности медицинской деятельности, поэтому ее осуществление без сбора такой информации невозможно. В связи этим проблема защиты персональных данных в сфере здравоохранения на сегодняшний день остается чрезвычайно актуальной.

Персональные данные могут быть подвержены различным угрозам, под которыми понимают совокупность условий и факторов, которые создают опасность несанкционированного, в том числе случайного доступа к ним при хранении или в процессе обработки в информационной системе, результатом чего могут стать те или иные неправомерные действия. В соответствии с действующим законодательством любой государственный (муниципальный) орган, а также юридическое или физическое лицо, осуществляющее сбор, обработку и хранение персональных данных, называется оператором. Обработкой персональных данных считаются любые действия, совершаемые с ними. В зависимости от цели, которую преследует оператор персональных данных, и его функциональных обязанностей, он может быть регистратором, который собирает данные и вводит их в базу данных, пользователем, которому эта информация необходима для осуществления своей профессиональной деятельности (например, врач, медицинская сестра, исследователь и др.), или относиться к «техническому персоналу», чья функция заключается в непосредственной работе с данными, например, их обезличивание, кодирование, систематизация (например, IT-специалист). Выделение таких категорий операторов представляется существенным для организации защиты персональных данных.

В соответствии с действующим законодательством обязанность по защите персональных данных лежит на их операторе.

В информационных системах выделяют 3 типа угроз для персональных данных (табл. 2):

Таблица 2.

Типы угроз персональным данным

Тип угроз	Характеристика типа угроз
1 тип	Связаны с возможностями системного программного обеспечения
2 тип	Связаны с возможностями прикладного программного обеспечения
3 тип	Связаны с причинами, не относящимися к программному обеспечению

В связи с неоднородностью персональных данных, различными по своей тяжести последствиями их утраты или изменения, а также сложностью предотвращению угроз для них разделены на 4 уровня: от наивысшего, до низшего. Такая классификация типов угроз для персональных данных и стратификация на четыре уровня их защищенности позволяет рационально использовать ресурсы, необходимые для осуществления мероприятий по их защите. Принципиальное отличие информационных медицинских технологий состоит в том, что при их использовании помимо данных о личности пациента (фамилия, имя, отчество, дата рождения, адрес проживания, паспортные данные и т.п.) проводится постоянный сбор и хранение информации о состоянии его здоровья в виде электронной истории болезни.

Система защиты информации должна состоять из 4 подсистем:
- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

Все оборудование, используемое с данной целью, должно проходить обязательную государственную сертификацию. Прикладная область информатики, занимающаяся вопросами обеспечения безопасности данных, носит название DLP (Data Loss/ Leakage Prevention). Специалисты в данной области выделяют 2 канала утечки информации — сеть и мобильные носители данных. Ее причинами могут быть следующие факторы: внешние (DoS-атака), внутренние (умышленные и неумышленные

действия сотрудников) и смешанные (внедрение вредоносного программного обеспечения через Web-браузеры или спам). До 90% причин утечек — внутренние. Специалисты в данной области признают, что обеспечить абсолютную защиту данных невозможно, поэтому вся деятельность в этом направлении сводится к максимальному снижению рисков. Ими предложено 3 подхода к созданию DLPсистем:

1) анализ контента (содержания получаемой и передаваемой информации) по специальному алгоритму с использованием ключевых слов;
2) грифование электронных документов специальными метками;
3) комбинация этих подходов.

Появлению любого правового документа предшествует прецедент, то есть значимое для общества событие. После осознания проблемы и выдвижения законодательных инициатив следует их длительное обсуждение и выполнение необходимых процедур, необходимых для принятия правовых актов. Все это приводит к тому, что законодательное регулирование, как правило, запаздывает, создавая на протяжении определенного времени «правовой вакуум» или не отвечает стремительно изменяющимся потребностям общества. Одним из примеров может служить требование получения информированного согласия на обработку персональных данных.

В настоящее время в Российской Федерации существует презумпция несогласия лица на любые действия с его персональными данными. Так, в соответствии с п. 8 ст. 10.1 Закона о персональных данных молчание или бездействие субъекта таких сведений ни при каких обстоятельствах не может считаться согласием на их обработку. Правда этот же Закон оговаривает особые случаи, к которым относят в том числе обработку данных в целях защиты жизни и здоровья граждан, при оказании медицинской помощи, в области обязательных видов страхования, проведении научных исследований.

В целом же защита персональных данных остается одним из наиболее болезненных вопросов, поскольку информация о состоянии здоровья граждан требует обеспечения наивысшего уровня защищенности. Вместе с тем в реальной практике такие мероприятия часто носят формальный характер.

Информированное согласие на сбор и обработку персональных данных далеко не всегда обеспечивает права пациента на конфиденциальность личной жизни и соблюдение врачебной тайны. Юридическая база, как правило, отстает от стремительного развития цифровых технологий и реагирует уже на состоявшиеся события, которые служат основой для разработки и принятия законодательных актов. Поэтому основу защиты персональных данных всё-таки должны составлять организационные и технические мероприятия, способные обеспечить повышенные стандарты безопасности и динамично развиваться, своевременно реагируя на неизбежное появление новых угроз, бурное развитие информационных технологий и достижения медицинской науки.

ГЛАВА 6. РАЗВИТИЕ ЦИФРОВЫХ КОМПЕТЕНЦИЙ ВРАЧА

Понятие цифровых компетенций врача весьма расплывчато. Единственное, что оно четко подразумевает — это уверенное взаимодействие с информационными технологиями, используемыми в клинической практике. Без владения цифровыми навыками квалифицированная деятельность в медицине сегодня вряд ли возможна. Цифровизация здравоохранения набирает обороты, прогрессируя от ставших обыденными электронных медицинских карт до внедрения нейросетей с искусственным интеллектом (ИИ) и технологий дополненной реальности в учебную практику.

По мере дигитализации отрасли здравоохранения все большее значение будет приобретать цифровая грамотность медицинского персонала. Прямо на наших глазах цифровые компетенции врачей начинают оказывать самое серьезнейшее влияние на лечебно-профилактическую работу, и эта тенденция только усилится в будущем. Цифровая грамотность (digital fluency) определяется набором знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий и ресурсов Интернета. Цифровые компетенции (digital competencies) лежат в основе цифровой грамотности и подразумевают под собой способность решать разнообразные задачи в области использования цифровых технологий. Под термином цифровые навыки (digital skills) принято понимать устоявшиеся, доведенные до автоматизма модели поведения, основанные на знаниях и умениях в области использования цифровых устройств, коммуникационных приложений и сетей для доступа к информации и управления ею. Данные навыки позволяют медицинским работникам создавать цифровой контент, обмениваться им, решая различные вопросы для того, чтобы сделать производственные процессы более эффективными.

Среди цифровых навыков выделяют пользовательские и профессиональные.

- Пользовательские цифровые навыки: базовые цифровые навыки, связанные с функциональной грамотностью

в использовании электронных устройств и приложений. Это навыки работы с файлами, устройствами, онлайн-сервисами и приложениями, умение печатать на клавиатуре.

- Специализированные профессиональные цифровые навыки, связанные с регулярным решением сложных профессиональных задач в цифровой среде; это как раз то, что лежит в основе высокотехнологичных процедур.

С одной стороны, работа в медицинской информационной системе, требует владения базовыми навыками, с другой стороны, зачастую врачам требуются гораздо более высокоуровневые компетенции, поскольку они могут заниматься написанием научных статей, ведут блоги в социальных сетях или какие-либо просветительские проекты. Врачам необходимо читать специальную литературу, осуществлять научный поиск, выполнять статистическую обработку медицинских данных. В плане специализированных навыков уместен пример с владением статистическими пакетами программ.

Есть несколько компетенций, которые важны для врачей всех специальностей. Чтобы использовать ресурсы цифровых платформ здравоохранения в полной мере, специалистам необходимо знать, как медицинские данные можно превратить в релевантную информацию. В последнее время из-за быстрого накопления «больших данных» в системе здравоохранения гораздо важнее уметь осуществлять быстрый поиск качественной информации, чем просто иметь академический опыт. Следовательно умение управлять организацией медицинских знаний становится все более актуальным. Приведём ряд универсальных компетенций врача, связанных с цифровой медициной.

1. Управление информацией и безопасность персональных данных: юридические формальные процедуры управления информацией, которые обеспечивают безопасность данных. Например, передача персональных данных пациентов с помощью цифровых технологий, общие протоколы обеспечения кибербезопасности внутри медицинского учреждения.

2. Использование цифровых систем и клиническая безопасность: использование электронных медицинских карт, выписка рецептов, прогнозирование вероятности системных ошибок, которые могут исказить назначения, знания об особенностях работы диагностических приборов и проблемах, связанных с ними. Правовая безопасность врача при использовании цифровых

платформ однозначно не гарантирована, так как нормативное регулирование не всегда поспевает за темпом внедрения новых медицинских технологий. По этой причине врачу крайне важно своевременно получать информацию о текущем состоянии дел в правовом поле.

3. Цифровая коммуникация: передача данных пациента, телемедицина, понимание возможностей и ограничений телемедицинской консультации.

4. Управление информацией и медицинскими знаниями: понимание степени качества различных источников информации, механизмов принятия решений с учетом имеющихся данных, знание основ анализа и интерпретации научных данных.

5. Ориентация на пациента: расширение прав и возможностей пациентов в контексте новых возможностей цифровых технологий, обучение пациентов использованию цифровых устройств для диагностики и лечения, предоставление пациентам качественных источников медицинской информации.

6. Быстрая адаптация к цифровым инновациям в здравоохранении: знание и понимание новых тенденций, подходов, технологий, которые входят в клиническую практику, проактивное их освоение.

Теперь ясно, что цифровые компетенции не только обеспечивают врачам возможность функционирования на качественно ином, т.е. более высоком уровне, оптимизируя свою деятельность, обеспечивая собственную безопасность, но и в корне изменяют их привычки и поведенческие паттерны.

Вызывает интерес следующий вопрос: не страдает ли качество медицинской помощи от отсутствия у врача цифровых навыков. В контексте цифровой медицины мы имеем дело с взаимодействием человека и компьютера, поэтому ошибки могут быть как со стороны медицинского работника, так и со стороны программного обеспечения.

Для того чтобы минимизировать общее число ошибок необходимо четкое соблюдение правил использования информационных технологий. Обучение медицинских работников позволяет сократить количество ошибок, связанных не со сбоями в работе оборудования, а с человеческим фактором, то есть некорректно или несвоевременно введенными данными, отсутствием реакции на предупреждения от системы, неиспользование возможностей программного обеспечения в полной мере, что встречается

гораздо чаще, чем технические сбои. Это также позволяет не полагаться на компьютер слишком сильно: например, ускорившееся развитие моделей медицинского ИИ требует тщательной проверки истинности выдаваемой нейросетью информации профессиональным экспертом.

Пока ещё цифровые навыки большинства врачей недостаточны для того, чтобы они могли стать полноценными пользователями и создателями цифрового пространства в медицине. Даже среди молодых специалистов, с детства использующих достижениями информационных технологий, уверенное владение цифровыми инструментами демонстрирует не более четверти аудитории. Зачастую врачи проходят формальное обучение, организованное силами производителя какого-либо программного продукта, используемого в медицинской организации. Такое обучение не позволяет получать навыки применения иных программ, которые им приходится осваивать самостоятельно.

В России, согласно опросу о цифровизации здравоохранения, проведенному ресурсом Врачи.РФ, 75,1% отмечают увеличение рабочей нагрузки после внедрения элементов Единого цифрового контура в работу; 61,8% респондентов отмечают, что Единый цифровой контур (ЕЦК) скорее усложняет работу с документами пациентов; 90% врачей отмечают, что есть необходимость дублировать электронную и медицинскую документацию. Такая статистика связана, в первую очередь, с отсутствием понимания у врачебного персонала возможностей и ограничений медицинских информационных систем (МИС), в то время как детальное и последовательное обучение могло бы существенно улучшить показатели.

Однако ежедневная рабочая нагрузка врачей крайне высока, и факультативное обучение использованию информационных технологий обычно мало востребовано, особенно специалистами, относящимися к ним критично. Поэтому базовые цифровые компетенции целесообразно осваивать в рамках обязательных курсов. Для закрепления полученных знаний и навыков желательно сочетать онлайн-курсы и очное обучение. Для разработки и реализации таких программ было бы полезно привлечь специалистов в области медицинской информатики и, при необходимости, экспертов в других смежных областях.

В настоящее время цифровизация здравоохранения в РФ только набирает обороты, и, несмотря на наличие большого

количества хорошо оснащенных медицинских центров, подготовленных специалистов, в масштабах страны предстоит еще много работы. По данным опроса на сайте Врачи.РФ, только 20% респондентов были удовлетворены цифровой зрелостью своей организации. Что касается обучения, менее 2% медицинских работников проходили целенаправленное обучение по цифровым навыкам, и только 6,9% всех опрошенных врачей целенаправленно обучались этим навыкам самостоятельно.

Важным образовательным ресурсом для врачей, независимо от специализации и региона, является портал непрерывного медицинского и фармацевтического образования edu.rosminzdrav.ru (НМФО). С 2022 г. на нем специально разработаны интерактивные образовательные модули (ИОМ), направленные на обучение врачей использованию МИС. Для обучения работе в "Единой цифровой платформе" разработано 8 цифровых модулей для медицинских работников разных специальностей: для врачей поликлиники, стационара, врачей-стоматологов, медицинских сестер, лаборантов и т.д. Эти образовательные элементы врачи могут осваивать прямо на своем рабочем месте, без необходимости выезда в образовательную организацию, что позволяет интегрировать обучение в их повседневную работу. Именно поэтому использование ИОМ обладает большим потенциалом для развития цифровых навыков работающих специалистов. Одним из путей развития цифровых навыков будущих врачей также является обучение студентов в вузе по отдельным программам.

Очень важным моментом является взаимодействие разработчиков МИС с конечным потребителем. Привлеченные к разработке врачи помогали бы находить наиболее удобные рабочие решения. В целом междисциплинарное сотрудничество медицинских работников является необходимым условием качественной разработки цифровых платформ в здравоохранении. Для повышения уровня оказания медицинской помощи врачам клинических специальностей необходимо сотрудничать с экспертами в области медицинской информатики, исследователями, инженерами медицинского оборудования и другими специалистами и принимать активное участие в дальнейших разработках в области медицины. В англоязычном пространстве сети Интернет есть объемные курсы по цифровому здравоохранению. Это крупные, длительные обучающие программы,

обычно состоящие из нескольких модулей (Coursera, Frauhofer Academy), однако для обычного врача, являющегося только пользователем уже внедренных цифровых технологий, подобное обучение часто избыточно.

Крайне важным моментом в обучении врачей является выделение на это достаточного количества времени и ресурсов. Обучение должно фокусироваться не только на функционале программного обеспечения (ПО), но и на клинической пользе, которую может получить бригада врачей или конкретный специалист от применения данного ПО. Некоторым врачам, у которых цифровые навыки в целом находятся на низком уровне, необходимо менторство со стороны специалистов в сфере IT или коллег. Организационный момент крайне важен для мотивации человека. При работе в мультидисциплинарной команде люди склонны более активно пользоваться компьютерными технологиями. Кроме того, если работа с МИС имеет качественное правовое регулирование, то врач работает с ней гораздо охотнее.

Уже сегодня в рамках отдельных специальностей наблюдается широкое внедрение в клиническую практику такого важного цифрового инструмента, как ИИ. Самыми перспективными сферами приложения медицинского ИИ являются автоматизированный анализ медицинских изображений и платформы поддержки принятия врачебных решений. С 2014 по 2021 годы рынок медицинского ИИ вырос в 11 раз (рис. 1):

Этот прирост вполне оправдан, ибо эти технологии позволят удовлетворить потребности клиницистов, которые не могли быть обеспечены доступными ранее материально-техническими или научными средствами (рис. 2).

Прирост стартапов в области ИИ в медицине быстро увеличивается, а рынок ИИ в здравоохранении испытывает среднегодовой прирост более 40%

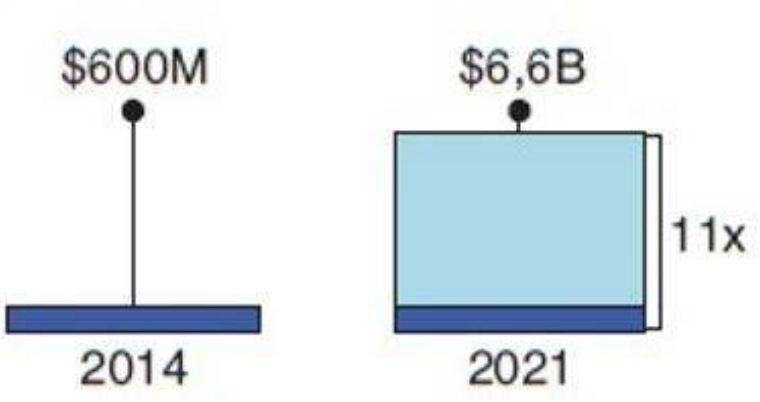

Рисунок 1. Прирост рынка медицинского ИИ за период 2014-2021 гг.

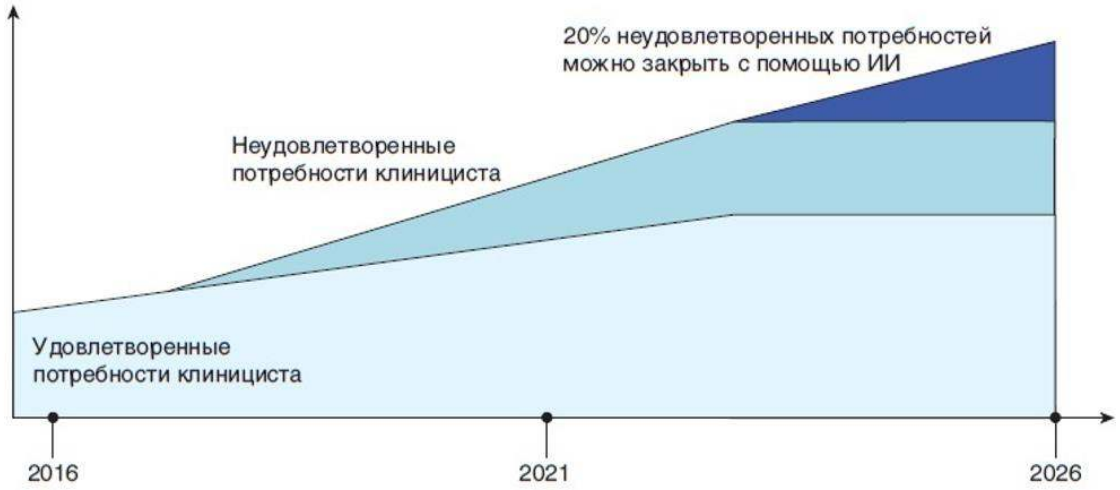

Рисунок 2. Динамика удовлетворения запросов клиницистов за счет использования платформ ИИ.

Использование ИИ в медицине имеет огромную перспективу. В целом мир движется к автоматизации множества рабочих процессов. Автоматизация в здравоохранении позволит освободить более трети рабочего времени специалистов, которые могут тратить его на иные, более творческие задачи, на коммуникацию с пациентом. Важно понимать, что системы с использованием ИИ не заменяют врача, а лишь автоматизируют часть его работы. При этом у врача освобождается ресурс на более качественную коммуникацию с пациентом, творческую работу, более тщательный анализ сложных случаев. Также невозможно не контролировать правильность работы информационных систем, что тоже будет задачей врача. Для этого врач должен понимать принцип работы, возможности и ограничения системы.

Неоднозначно и отношение врачей к ИИ: многих из них беспокоит, что искусственный интеллект заменит их функции полностью, и их собственная экспертиза будет обесцениваться, изменятся отношения врача и пациента. При этом качество систем с использованием ИИ и информативность его применения очень сильно зависит и от самих специалистов здравоохранения как от основных поставщиков медицинских данных, на которых обучается ИИ. Таким образом, очень важна вовлеченность самих врачей в развитие подобных систем, а для этого они должны видеть, как краткосрочные преимущества для своей работы (например, участие в научных публикациях), так и долгосрочные (оптимизация своей работы, повышение качества

помощи пациентам). В этом контексте огромное значение имеет роль личности врача как лидера в освоении новых технологий и демонстрации коллегам того, как их лучше использовать.

Все это не может быть достигнуто без высокого уровня цифровой грамотности врачей, которые должны выступать компетентными заказчиками инновационных моделей ИИ для обеспечения более высокого качества своей работы и квалифицированными пользователями, которые могут в полной мере использовать функционал тех нейросетей, которые будут разработаны для облегчения их работы.

Врачу-лидеру важно формировать своё цифровое портфолио, которое представляет собой электронную коллекцию профессиональных достижений и документов и которая включает сведения об образовании, сертификаты, публикации, опыт работы, отзывы пациентов и другие важные материалы. Цифровое портфолио помогает врачу демонстрировать свою квалификацию потенциальным работодателям, коллегам и пациентам. Создание такого портфолио требует структурированного подхода к сбору информации и использования удобных платформ для его размещения (например, специализированные сайты или личные веб-страницы).

Врачи могут использовать следующие цифровые технологии для демонстрации своих профессиональных достижений:

- Личные веб-сайты: Создайте персональный сайт с разделами, посвященными образованию, опыту работы, публикациям, сертификатам и достижениям.
- Социальные сети: Используйте профессиональные платформы вроде LinkedIn, чтобы делиться своими успехами, участвовать в обсуждениях и привлекать внимание потенциальных работодателей.
- Электронное портфолио: Создавайте электронные портфолио с помощью специализированных сервисов, таких как Google Sites, Wix или WordPress, где можно разместить документы, видео и презентации.
- Видео-презентации: Записывайте видео-обзоры своих проектов, выступлений на конференциях или операций, которые вы провели успешно.
- Публикация статей: Публикуйте статьи в научных журналах и блогах, а также делитесь ссылками на них через социальные сети и свой личный сайт.

- Онлайн-курсы и вебинары: Участвуйте в онлайн-курсах и вебинарах, а затем добавляйте полученные сертификаты в свое цифровое портфолио.
- Мобильные приложения: Используйте медицинские мобильные приложения для ведения электронных медицинских карт, записи результатов исследований и обмена данными с коллегами.
- Телемедицина: Применяйте телемедицинские сервисы для консультаций с пациентами и коллегами, что может быть продемонстрировано как часть вашего опыта.

Все перечисленные инструменты помогут врачам эффективно представить свои навыки и достижения перед широкой аудиторией.

Итак, цифровые компетенции должны стать наиважнейшей составляющей профиля личности российского врача будущего. Именно они выступают лимитирующими факторами ускоренной цифровизации отечественного здравоохранения. Развитие цифровых компетенций является одним из приоритетных направлений медицинского образования. Для глубокого укоренения цифровых технологий в практическом здравоохранении необходима полноценная подготовка в этом направлении, в том числе предусматривающая стимулирование формирования лидерских качеств у врачей всех специальностей.

ЗАКЛЮЧЕНИЕ

В заключение важно подчеркнуть, что цифровая трансформация играет ключевую роль в развитии современной медицины и профессиональной деятельности врачей. Подытожим те причины, почему она так важна:

- Улучшение качества медицинской помощи. Цифровые технологии позволяют врачам быстрее получать доступ к актуальной информации, анализировать данные пациентов, применять искусственный интеллект для диагностики и лечения. Это способствует более точному и своевременному принятию решений, что повышает качество оказываемой помощи.
- Оптимизация рабочих процессов. Автоматизация рутинных задач, таких как ведение документации, назначение анализов и запись на прием, освобождает время врачей для более важных аспектов их работы. Электронные медицинские карты и системы управления ресурсами помогают упорядочить работу клиники и повысить ее эффективность.
- Доступность медицинских услуг. С развитием телемедицины врачи могут консультировать пациентов удаленно, что особенно важно для жителей отдаленных регионов или людей с ограниченными возможностями передвижения. Это делает медицинскую помощь более доступной и удобной.
- Обучение и профессиональное развитие. Онлайн-курсы, вебинары и образовательные платформы предоставляют врачам возможность постоянно повышать свою квалификацию без отрыва от основной работы. Доступ к международным ресурсам позволяет оставаться в курсе последних тенденций и инноваций в медицине.
- Безопасность данных. Современные системы защиты данных обеспечивают конфиденциальность и безопасность медицинской информации. Врачи могут быть уверены, что данные пациентов защищены от несанкционированного доступа.
- Интеграция с другими специалистами. Цифровые платформы позволяют врачам легко взаимодействовать с коллегами, обмениваться опытом и знаниями, а также совместно работать

над сложными случаями. Это способствует междисциплинарному подходу к лечению и улучшению результатов.

- Исследования и инновации. Использование больших данных и искусственного интеллекта открывает новые возможности для проведения клинических исследований и разработки инновационных методов лечения. Врачи могут активно участвовать в этих процессах, способствуя прогрессу в области здравоохранения.

Таким образом, цифровая трансформация не только улучшает повседневную работу врачей, но и расширяет их возможности для профессионального роста и развития медицины в целом.

Что касается перспектив цифрового лидерства в медицине то следует отметить, что оно обещает значительные изменения в том, как будет организована медицинская практика, как будут приниматься решения и как пациенты получат доступ к медицинским услугам. Вот основные направления, по которым ожидается развитие:

- Искусственный интеллект (ИИ) станет ключевым инструментом для анализа больших объемов данных, диагностики заболеваний, прогнозирования исходов лечения и персонализации терапии. ИИ сможет помогать врачам принимать более обоснованные клинические решения, сокращая ошибки и повышая точность диагнозов.
- Дистанционные консультации, мониторинг состояния здоровья пациентов и предоставление медицинских услуг через интернет станут нормой. Это позволит улучшить доступность медицинской помощи, особенно в регионах с недостатком специалистов.
- Устройства интернета вещей IoT, такие как носимые датчики, умные часы и домашние медицинские приборы, будут собирать данные о состоянии пациента в реальном времени. Эти данные позволят врачам оперативно реагировать на изменения в здоровье пациента и корректировать планы лечения.
- Блокчейн-технологии обеспечат безопасное хранение и передачу медицинских данных между различными учреждениями и врачами. Это повысит прозрачность и доверие к системе здравоохранения, снизив риск утечек и мошенничества.
- Анализ генома каждого пациента позволит разрабатывать индивидуальные подходы к диагностике и лечению.

Персонализация медицины приведет к созданию более эффективных терапевтических стратегий и снижению побочных эффектов лекарств.

- Роботизированные хирургические системы. Роботы-хирурги уже используются в некоторых операциях, и их применение будет расширяться. Они смогут выполнять сложные процедуры с высокой точностью, минимизируя риски для пациентов.
- Образование и непрерывное обучение. Виртуальная реальность и симуляторы будут использоваться для обучения студентов-медиков и повышения квалификации практикующих врачей. Это обеспечит более реалистичную подготовку и улучшение практических навыков.
- По мере внедрения новых технологий возникнет необходимость в разработке этических стандартов и правовых рамок для их применения. Вопросы конфиденциальности, безопасности данных и ответственности за использование ИИ и других цифровых инструментов потребуют тщательного регулирования.
- Будут развиваться партнерские отношения между медицинскими учреждениями, технологическими компаниями и исследовательскими центрами. Совместные проекты позволят ускорить внедрение инноваций и распространение лучших практик.
- Цифровое лидерство в медицине будет направлено на повышение удовлетворенности пациентов. Пациенты будут иметь больше контроля над своим здоровьем благодаря доступу к данным и возможностям самостоятельного мониторинга своего состояния.

В итоге будущее цифрового лидерства в медицине обещает значительное улучшение качества и доступности медицинских услуг, повышение эффективности работы врачей и ускорение прогресса в лечении различных заболеваний.

ЛИТЕРАТУРА

1. Федеральный закон № 152-ФЗ от 27 июля 2006 г. (ред. от 02.07.2021) «О персональных данных».
2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
3. Федеральный закон от 30.12.2020 № 159-ФЗ «О внесении изменений в закон «О персональных данных».
4. Постановление Правительства РФ от 05.05.2018 № 555 (ред. от 02.02.2019) «О Единой государственной информационной системе в сфере здравоохранения»).
5. Постановление Правительства РФ от 28.11.2011 г. № 977 (ред. от 24.06.2021) «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
6. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
7. ГОСТ Р 50922-2006 «Защита информации: основные термины и определения». М.: Стандартинформ, 2008; 8 с.
8. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
9. Аксенова Е.И., Шкрумяк А.Р. Кадры здравоохранения в условиях внедрения цифровых систем. Бюллетень национального научно-исследовательского института общественного здоровья имени Н.А. Семашко. 2021. № 4. Р. 130-137. https://doi.org/10.25742/NRIPH.2021.04.018
10. Бердутин, В.А., Романова, Т.Е., Романов, С.В., Абаева, О.П., Дзюбак С.А. (2024) Понятийный аппарат, связанный с цифровизацией здравоохранения. Учебно-методическое пособие. М.: ФГБУ ГНЦ ФМБЦ им. А.И. Бурназяна ФМБА России. 68 с. ISBN: 978-5-93064-287-2
11. Бихатова Э.Т., Иванчук О.В. Проблема формирование цифровых компетенций у студентов медицинских вузов. ЦИТИСЭ. 2021. Т. 30, № 4. С. 595-605. https://doi.org/10.15350/2409-7616.2021.4.55
12. Всеобщая декларация о биоэтике и правах человека» (ЮНЕСКО, 2005). https://www.un.org/ru/documents/decl_conv/declarations/bioethics_and_hr.shtml
13. Демина Э.А., Карасева Л.А., Двойников С. И., Сиротко М.Л. Оценка эффективности программы «автоматизированное рабочее место старшей медицинской сестры». Проблемы социальной гигиены, здравоохранения и истории медицины. 2020. Т. 28, № 4. С. 610-615. https://doi.org/10.32687/0869-866X-2020-28-4-610-615

14. Дзюбак, С.А., Романова, Т.Е., Бердутин, В.А. (2024) Интеллектуальная компьютерная система динамической маршрутизации пациентов поликлиники. Главврач. №9, С. 6-17. doi: 10.33920/med-03-2409-01
15. Дудин М.Н., Голышко П.В., Вашаломидзе Е.В., Гурцкой Д.А., Гурцкой Л.Д. Развитие цифровых компетенций медицинских работников в контексте всеобщей цифровизации российского здравоохранения. Проблемы социальной гигиены, здравоохранения и истории медицины. 2022. Т. 30, № 5. С. 843-852. https://doi.org/10.32687/0869-866X-2022-30-5-843-852
16. Карпов О. Э., Субботин С. А., Шишканов Д. В., Замятин М. Н. Цифровое здравоохранение. Необходимость и предпосылки. Врач и информационные технологии. 2017; (3): 6-22.
17. Коленникова О.А. Владение медицинскими специалистами цифровыми технологиями. Народонаселение. 2022. Т. 25, № 3. С. 189-199. https://doi.org/10.19181/population.2022.25.3.15
18. Монаков Д.М., Шадеркина В.А., Рева С.А., Грицкевич А.А. Защита персональных данных пациентов при использовании телемедицинских технологий в период пандемии COVID-19. Российский журнал телемедицины и электронного здравоохранения 2021;7(4):48-57; https://doi.org/10.29188/2712-9217-2021-7-4-48-57
19. Нежметдинова Ф. Т., Гурылёва М. Э. Цифровизация медицины и этические проблемы в условиях пандемии COVID-19. Медицинская этика. MEDET.RSMU.PRESS. 3; 2021; 17-23. https://doi.org/10.24075/medet.2021.023
20. Петров И. М., Спадерова Н. Н., Мальцева О. Н., Егоров Д. Б., Петров Д. И. Этические вызовы внедрения «цифрового здравоохранения». Медицинская наука и образование Урала. 2019; (4): 203-20
21. Портал непрерывного медицинского и фармацевтического образования Минздрава России. URL: https://edu.rosminzdrav.ru/
22. Совет Наффилда. Публикации. Здоровье и общество. COVID-19. https://www.nuffieldbioethics.org/ topics/health-and-society/covid-19
23. Столяр В.П., Крайнюков П.Е., Калачев О.В. Цифровая трансформация здравоохранения и ведомственной медицины. М.: Планета, 2020;200 с.
24. Шайдуллина В.К. Большие данные и защита персональных данных: основные проблемы теории и практики правового регулирования. Общество: политика, экономика, право 2019;66(1):51-55.
25. Ahuja A.S. The impact of artificial intelligence in medicine on the future role of the physician. Peer J. 2019. N 7. P: e7702. https://doi.org/10.7717/peerj.7702
26. Aulenkamp J., Mikuteit M., Löffler T., Schmidt J. Overview of digital health teaching courses in medical education in Germany in 2020. GMS J Med Educ. 2021. Vol. 38, N 4. P. Doc80. https://doi.org/10.3205/zma001476
27. Banerjee R., George P., Priebe C., Alper E. Medical student awareness of and interest in clinical informatics. J Am Med Inform Assoc. 2015. Vol. 22 (e1). P: e42-7. https://doi.org/10.1093/jamia/ocu046
28. Buck C., Doctor E., Hennrich J., Jöhnk J., Eymann T. General practitioners' attitudes toward artificial intelligence-enabled systems: interview study. J Med Internet Res. 2022. Vol. 24, N 1. P. e28916. https://doi.org/10.2196/28916
29. Coravos A., Goldsack J. C., Karlin D. R., Nebeker C., Perakslis E., Zimmerman N., Erb M. K. Digital Medicine: A Primer on Measurement Digit Biomark 2019; 3: 31-71 https://doi.org/10.1159/000500413 30

30. Cortellazzo L., Bruni E., Zampieri R. The role of leadership in a digitalized world: a review. Front Psychol. 2019. Vol. 10. P. https://doi.org/193810.3389/fpsyg.2019.01938
31. Cullen R., Clark M., Esson R. Evidence-based information-seeking skills of junior doctors entering the workforce: an evaluation of the impact of information literacy training during pre-clinical years // Health Info Libr J. 2011. Vol. 28, N 2. P. 119-129. https://doi.org/10.1111/j.1471-1842.2011.00933.x
32. Detmer D.E. Interprofessional clinical informatics education and practice: Essentials for learning healthcare systems worldwide. J Interprof Care. 2017. T. 31, № 2. C. 187-189. https://doi.org/10.1080/13561820.2016.1250554
33. di Giacomo D., Vittorini P., Lacasa P. Editorial: digital skills and life-long learning: digital learning as a new insight of enhanced learning by the innovative approach joining technology and cognition // Front Psychol. 2018. Vol. 9. P. 2621. https://doi.org/10.3389/fpsyg.2018.02621
34. European Health Parliament. Committee on digital skills for health professionals 2016. URL: https://www.healthparliament.eu/wp-content/uploads/2017/09/Digital-skills-for-health-professionals.pdf
35. Foadi N., Varghese J. Digital competence — a key competence for todays and future physicians // J Eur CME. 2022. Vol. 11, N 1. P. 1. https://doi.org/10.1080/21614083.2021.2015200
36. Gesualdo F., Daverio M., Palazzani L., et al. Digital tools in the informed consent process: a systematic review. BMC Med Ethics. 2021;22:18 https://doi.org/10.1186/s12910–02100585–8
37. Inan O.T., Tenaerts P., Prindiville S.A. et al. Digitizing clinical trials. npj Digit. Med. 2020 Jul 31;3:101. https:// doi.org/10.1038/s41746–020–0302-y
38. Jidkov L., Alexander M., Bark P., Williams J.G., Kay J., Taylor P. et al. Health informatics competencies in postgraduate medical education and training in the UK: a mixed methods study // BMJ Open. 2019. Vol. 9, N 3. P. e025460. https://doi.org/10.1136/bmjopen-2018-025460
39. Kim M.O., Coiera E., Magrabi F. Problems with health information technology and their effects on care delivery and patient outcomes: a systematic review. Journal of the American Medical Informatics Association. 2017. Vol. 24. N 2. P. 246-250. https://doi.org/10.1093/jamia/ocw154
40. Kuhn S. et al. Digital skills for medical students — qualitative evaluation of the curriculum 4.0 “Medicine in the digital age”. GMS journal for medical education. 2020. Vol. 37, N 6. P. Doc60.
41. Nezhmetdinova F. Global challenges and globalization of bioethics. Croatian Medical Journal, 2013; 54(1): 8385.
42. Rahal R.M., Mercer J., Kuziemsky C., Yaya S. Factors affecting the mature use of electronic medical records by primary care physicians: a systematic review. BMC Med Inform Decis Mak. 2021. Vol. 21, N 1. P. 67. https://doi.org/10.1186/s12911-021-01434-9
43. Reich J.L.K., Khakhria K. NHS must lead innovation in digital medicine. BMJ. 2019. Vol. 365. P. l1944. https://doi.org/10.1136/bmj.l1944
44. Roda S. Digital skills for doctors — explaining European doctors’ position // J Eur CME. 2021. Vol. 10, N 1. P. 1. https://doi.org/10.1080/21614083.2021.2014097

ПРИЛОЖЕНИЕ.
ТЕСТОВЫЕ ВОПРОСЫ

1. Что такое телемедицина?

A. Удаленное наблюдение за состоянием пациента с использованием мобильных устройств.
B. Метод дистанционного общения врача с пациентом посредством телекоммуникационных технологий.
C. Система хранения электронных медицинских записей.

Правильный ответ: B

2. Как называется система, позволяющая хранить и обрабатывать медицинские данные пациента?

A. Электронная медицинская карта (ЭМК).
B. Медицинская информационная система (МИС).
C. Телеметрическая система.

Правильный ответ: A

3. Какой инструмент используется для автоматического анализа медицинских изображений?

A. Искусственный интеллект (ИИ).
B. Электронная почта.
C. Телефония.

Правильный ответ: A

4. Что означает термин «интернет вещей» (IoT)?

A. Сеть взаимосвязанных физических объектов, оснащённых технологиями для взаимодействия друг с другом и внешней средой.
B. Платформа для видеоконференцсвязи.
C. Технология шифрования данных.

Правильный ответ: A

5. Каким способом врач может получить доступ к результатам лабораторных исследований пациента?

A. Через электронную медицинскую карту.
B. Только при личном визите пациента.

C. Через телефонный звонок в лабораторию.

Правильный ответ: A

6. Что такое блокчейн в контексте здравоохранения?

A. Распределённый реестр транзакций, обеспечивающий безопасность и прозрачность передачи данных.
B. Программное обеспечение для создания сайтов.
C. Мобильное приложение для мониторинга артериального давления.

Правильный ответ: A

7. Какие устройства относятся к категории «носимых технологий»?

A. Смартфоны и планшеты.
B. Умные часы и фитнес-браслеты.
C. Лампочки и розетки.

Правильный ответ: B

8. Что такое big data в медицине?

A. Большие объемы данных, собираемых из разных источников, для анализа и принятия решений.
B. Облачное хранилище для медицинских файлов.
C. Сервис для видеозвонков.

Правильный ответ: A

9. Как называется технология, используемая для виртуальной реальности в обучении врачей?

A. VR (Virtual Reality).
B. GPS-навигация.
C. Социальные сети.

Правильный ответ: A

10. Что такое «цифровой двойник» пациента?

A. Копия медицинского паспорта пациента в электронном формате.
B. Виртуальный аналог пациента, созданный на основе его медицинских данных для моделирования и прогнозирования.
C. Идентификационный номер пациента в базе данных.

Правильный ответ: B

11. Как называется метод дистанционного наблюдения за состоянием пациента?

A. Телеаудитория.
B. Телеметрия.
C. Интернет-магазин.

Правильный ответ: B

12. Что такое EHR (Electronic Health Record)?

A. Электронная медицинская карта.
B. Программа для планирования рабочего графика врача.
C. Сайт для поиска работы врачом.

Правильный ответ: *A*

13. Как называется программное обеспечение, которое помогает врачам принимать клинические решения на основе анализа данных?

A. CDSS (Clinical Decision Support System).
B. CRM-система.
C. Антивирусное ПО.

Правильный ответ: A

14. Что такое м-Health?

A. Приложения и услуги для мобильного здравоохранения.
B. Онлайн-магазины медицинских товаров.
C. Платежные системы для оплаты медицинских услуг.

Правильный ответ: A

15. Как называется устройство, которое измеряет уровень глюкозы в крови у диабетиков?

A. Глюкометр.
B. Термометр.
C. Шагомер.

Правильный ответ: A

16. Что такое роботизированная хирургия?

A. Хирургическое вмешательство, выполняемое роботом под контролем хирурга.
B. Лечение пациентов с помощью роботов-помощников.

C. Использование робота для доставки медикаментов пациенту.

Правильный ответ: A

17. Как называется платформа для дистанционного обучения врачей?

A. LMS (Learning Management System).
B. ERP-система.
C. CMS (Content Management System).

Правильный ответ: A

18. Что такое HIPAA?

A. Закон США о защите конфиденциальности и переносимости медицинской информации.
B. Международная организация здравоохранения.
C. Медицинский журнал.

Правильный ответ: A

19. Как называется программа, которая помогает врачам вести учет пациентов и назначений?

A. EMR (Electronic Medical Records).
B. Веб-браузер.
C. Офисное ПО.

Правильный ответ: A

20. Что такое биосенсоры?

A. Устройства, измеряющие физиологические параметры организма.
B. Камеры видеонаблюдения.
C. Системы кондиционирования воздуха.

Правильный ответ: A

21. Как называется система, которая автоматически назначает лекарства на основании диагноза?

A. Автоматизированная система назначения препаратов.
B. Автоматический дозатор лекарств.
C. Аптечный киоск.

Правильный ответ: A

22. Что такое облачные вычисления в медицине?

A. Хранение и обработка медицинских данных на удаленных серверах.
B. Разработка мобильных приложений.
C. Проведение видеоконференций.

Правильный ответ: A

23. Как называется технология, использующая радиочастотные метки для отслеживания медицинских приборов?

A. RFID (Radio Frequency Identification).
B. Wi-Fi роутер.
C. GPS-трекер.

Правильный ответ: A

24. Что такое e-Prescription?

A. Электронный рецепт.
B. Электронная почта.
C. Электронный кошелек.

Правильный ответ: A

25. Как называется сервис, позволяющий пациентам записываться на приём к врачу онлайн?

A. Онлайн-запись на приём.
B. Интернет-магазин.
C. Платёжная система.

Правильный ответ: ◠

Формат 60x90/16, объём 4 усл. печ. л. Бумага 80 г/м^2 офсетная.
Гарнитура Times New Roman. Тираж 1000 экз. Заказ № Н982.

Отпечатано в типографии ФГБУ ГНЦ ФМБЦ
им. А.И. Бурназяна ФМБА России.
123098 Москва, ул. Живописная, 46. Тел.: +7 (499) 190-93-90.
rcdm@mail.ru, lochin59@mail.ru
www.fmbafmbc.ru