**Автоматизированное рабочее место медицинского работника**

Необходимо знать: понятие автоматизированного рабочего места, общие принципы его создания, требования к организации; функции АРМ; классификацию АРМ сотрудников МО; понятие электронной истории болезни, концептуальная основа и технологии построения электронных историй болезни.

Необходимо уметь: определять класс АРМ сотрудника МО, указывать функции заданного АРМ;  уметь работать с готовой базой электронных историй болезни, вносить новые данные в базу и редактировать их.

Автоматизированное рабочее место (АРМ) - комплекс средств вычислительной техники и [программного обеспечения](http://www.pandia.ru/text/category/programmnoe_obespechenie/), располагающийся непосредственно на рабочем месте сотрудника и предназначенный для автоматизации его работы в рамках специальности.

Создание АРМ значительно улучшает качество лечебно-диагностической помощи. Сокращает время, затрачиваемое на оформление документации, позволяя уделять больше внимания работе с пациентами.

       Существует четыре общих принципа создания АРМ:

Системность: АРМ должно представлять собой систему взаимосвязанных компонентов, при этом структура АРМ должна строго соответствовать тем функциям, для выполнения которых создается данное автоматизированное рабочее место. Гибкость: данный принцип предполагает возможность модернизации АРМ, для этого все подсистемы рабочего места выполняются в виде отдельных легко заменяемых модулей, а для того, чтобы при замене не возникало проблем несовместимости, все элементы должны быть стандартизованы. Устойчивость: АРМ должно выполнять свои функции независимо от воздействия как внутренних, так и внешних факторов, при возникновении сбоев работоспособность системы должна быстро восстанавливаться. Эффективность: затраты на создание и эксплуатацию системы не должны превышать выгоду от ее использования.

       К автоматизированному рабочему месту предъявляются следующие требования:

полнота удовлетворения информационных потребностей пользователя (например, АРМ должно предоставлять доступ к различной справочной информации, руководствам по специальности и т. д.); минимальное время ответа на запросы пользователя, чем быстрее получена информация, тем выше ее ценность; адаптация к уровню подготовки пользователя и специфике выполняемых действий; возможность быстрого обучения пользователя основным приемам работы; надежность и простота обслуживания; дружественный интерфейс (работа с АРМ должна быть комфортной для пользователя); возможность работы в составе вычислительной сети (наличие коммуникаций объединяет АРМы в АСУ).

При создании автоматизированного рабочего места конкретного сотрудника, прежде всего, необходимо определить круг его должностных обязанностей, перечень наиболее типичных манипуляций, выполняемых на рабочем месте и потребность в той или иной информации. Следующим шагом является выбор функций, которые могут быть автоматизированы. На основе этих сведений создается АРМ с характерным набором технических и программных средств, наиболее полно отвечающее потребностям работника.

В настоящее время разработаны автоматизированные рабочие места практически для всех, нуждающихся в них, сотрудников лечебно-профилактических учреждений. Так существуют АРМ руководителя, сотрудника административно-хозяйственных служб (бухгалтера, специалиста по кадрам, юриста, секретаря и т. д.), АРМ врачей различных специальностей, медрегистратора, старшей сестры, постовой сестры и т. д.

Можно выделить несколько основных функций АРМ.

Регистрация пациентов (в АРМ медицинской сестры регистратуры, приемного отделения) и направление на обследование, к врачам-специалистам и на госпитализацию (в АРМ врача, заведующего отделением, главного врача и его заместителя, главного специалиста). Ведение медицинской документации. Эта функция реализуется в большинстве АРМ медицинских работников. Она включает обеспечение ввода, коррекции и хранения данных. Специальный модуль обеспечивает доступ к личному архиву и общим архивным данным с целью поиска прецедентов, что особенно важно при диагностике редких и сложных случаев заболеваний и выборе оптимальной для конкретного случая схемы лечения. Сортировка заявок в АРМ врачей, фельдшеров и медицинских сестер: в системе [скорой медицинской помощи](http://www.pandia.ru/text/category/skoraya_meditcinskaya_pomoshmz/), при телемедицинском консультировании, массовом поражении в чрезвычайных ситуациях и военно-полевых условиях. Планирование профилактических эпидемиологических мероприятий ([вакцинации](http://www.pandia.ru/text/category/vaktcina/), иммунизации) и контроль их выполнения в установленные сроки (в АРМ медицинской сестры прививочного кабинета). Модуль вакцинации и иммунизации должен включать медицинские показания и противопоказания к проведению прививок как постоянного, так и временного характера (например, эпидемиологическая обстановка в регионе, недавно перенесенное пациентом заболевание, выраженные [аллергические](http://www.pandia.ru/text/category/allergiya/) реакции в [анамнезе](http://www.pandia.ru/text/category/anamnez/) и т. д.). Этот АРМ строится в соответ­ствии с установленными нормативными требованиями, включая автоматическое формирование журнала прививочного кабинета. Планирование диспансерных осмотров. Это функция АРМ врача поликлиники (общей практики, участкового, специалистов). Поддержка лечебно-диагностических мероприятий. В АРМ врачей эта функция включает компьютерную диагностику, прогнозирование осложнений и динамики патологического процесса, выбор плана обследования и лечения (на основе утвержденных для конкретной патологии стандартов). Поддержка процесса выбора лечебной тактики предусматривает прогностическую оценку предлагаемого подхода, а конкретные методы лечения - учет показаний, противопоказаний, ограничений, совместимости и побочных эффектов препаратов для конкретного больного, расчет дозировок, ингредиентного баланса жидкостей и парентерального питания в перерасчете на массу или поверхность тела. При планировании оперативного вмешательства проводится автоматическая оценка риска предполагаемого исследования с учетом критерия альтернативы, обусловленного тяжестью состояния. Обработка данных и ведение электронного документооборота при проведении лабораторных, функциональных, радиологических и инструментальных исследований, в том числе с использованием программно-аппаратных комплексов. Поддержка [лабораторной диагностики](http://www.pandia.ru/text/category/laboratornaya_diagnostika/) включает оценку результатов исследований в сравнении с нормальными половозрастными значениями показателей, при учете установленного или предполагаемого диагноза и тяжести состояния, а также контроль качества исследований для оценки воспроизводимости, точности, правильности получаемых результатов. Поддержка функциональной и [лучевой диагностики](http://www.pandia.ru/text/category/luchevaya_diagnostika/) в рамках соответствующих АРМ включает: а) проведение расчетов (например, при анализе медицинских сигналов); б) сравнительный анализ физиологических параметров в разные возрастные периоды жизни и при различной патологии, масштабирование и контрастирование изображений, их наложение и сопоставление за различные временные интервалы, т. е. сравнение различных наблюдаемых паттернов (образов) с возможностью их представления в графической форме. Возможен просмотр как отдельных хранимых изображений, так и видеорядов, характеризующих процесс в динамике. Поддержка врачебных решений в процессе контроля мониторируемых показателей физиологического состояния организма. Непрерывный или дискретный контроль параметров жизненно важных систем организма с учетом диагноза и тяжести состояния пациента при одновременном анализе предшествующих и текущих записей в БД позволяет повысить эффективность поддержки принятия врачом оперативных решений. Компьютерное экспериментирование в фармакологии при создании новых фармакологических препаратов и при анализе взаимодействия лекарственных средств между собой. Виртуальный аспект процесса разработки новых медикаментов предполагает использование БД имеющихся фармакологических средств, включающее полный спектр их структуры и физико-химических свойств. Это необходимо для определения будущей реакционной способности метаболита, оценки потенциальной биотрансформации веществ, прогнозирования антипродуктивных качеств лекарственных препаратов и т. д. Аналогичным образом на основании знаний о химических и физических свойствах препаратов обеспечивается анализ взаимодействия лекарственных средств между собой. Поддержка организационных решений, включая прогнозирование и медико-тактические решения в чрезвычайных ситуациях. Медико-статистическая обработка данных. Эта функция должна быть предусмотрена в любом АРМ, но только в АРМ врача статистика является основной наряду с поддержкой базы медико-статистических данных. Расчет стоимости консультаций, обследования и лечения. Эта функция может осуществляться при необходимости на любом АРМ, но является основной для АРМ экономиста МО, в котором обычно предусмотрены возможности для углубленного [экономического анализа](http://pandia.ru/text/category/analiz_yekonomicheskij/) [деятельности медицинского](http://www.pandia.ru/text/category/deyatelmznostmz_meditcinskih_organizatcij/) учреждения, специальных служб или системы здравоохранения. Доступ к информационным ресурсам и дистанционный обмен данными. Эта функция предполагает возможность: а) обращения к разнообразным базам медицинских данных внутри учреждения (включая БД других АРМ), в специализированной корпоративной сети, в Интернете; б) обмена данными с использованием wifi-технологий в целях телеконсультирования и интерактивного аудио/видеообмена при видеоконсультациях.

Как видно из изложенного, АРМ медицинского работника - это общее понятие, объединяющее большой ряд АРМ, специализированных в соответствии с профилем деятельности работника. Почти любые проблемно-ориентированные АРМ могут функционировать самостоятельно или в составе ИМС.

Классификация автоматизированных рабочих мест в здравоохранении

Автоматизированные рабочие места классифицируют по разным критериям: назначению, технологии построения и т. д.

Рассмотрим классификацию АРМ, используемых в [медицинских учреждениях](http://pandia.ru/text/category/meditcinskie_tcentri/), в соответствии с их предназначением. Они подразделяются на три класса, внутри которых выделяют еще по несколько подклассов.

Медико-технологические:

клинические - АРМ врачей лечебных отделений, врачей - консультантов, фельдшеров, медицинских сестер; функциональные, радиологические, лабораторные - АРМ врачей функциональной диагностики, радиологических отделений, клинико-биохимических лабораторий и др.; фармакологические - АРМ специалистов, осуществляющих разработку лекарственных средств.

Организационно-технологические:

организационно-клинические - АРМ заведующих отделениями, заместителей главных врачей по лечебной работе, главных специалистов; телемедицинские - АРМ сотрудников, обеспечивающих проведение телеконсультаций.

Административные:

административно-управленческие - АРМ главных врачей, руководителей органов управления здравоохранением всех уровней; медико-статистические - АРМ сотрудников организационно-методических отделов и отделов статистики МО; медико-экономические - АРМ заместителей главных врачей МО по экономике, сотрудников экономических подразделений органов управления здравоохранением.

Рассмотрим один из видов АРМ – интеллектуальное АРМ.

Интеллектуальное АРМ - это программный продукт, в котором некоторая часть или все модули поддержки процесса принятая решений реализованы с использованием систем, основанных на знаниях (экспертных и(или) литературных). Такое АРМ позволяет осуществлять содержательный (в отличие от формального) анализ данных и предоставлять врачу объяснение предложенного решения, учитывающее его профессиональный уровень.

Все сведения, сообщаемые экспертом или извлекаемые из литературных источников при создании интеллектуального АРМ, должны быть проверены на внутреннюю непротиворечивость, полноту и соответствие реальной врачебной практике с учетом предполагаемого использования конкретного АРМ. Для этого можно осуществлять сопоставление с реальными медицинскими картами (историями болезни), описывающими результаты исследований и их медицинскую интерпретацию. Проверку полноты и избыточности списка заболеваний и состояний, а также используемой терминологии проводят путем формального сравнения фраз из предложенного экспертом списка с реальными врачебными заключениями. Для этого выписываются фразы из реальных заключений, не вошедшие в список возможных заключений (это носит название предположительного нарушения полноты), и фразы из списка, не встретившиеся в реальных заключениях (это носит название нарушения неизбыточности).

Особенно важна проверка на соответствие заключения и клинического описания. При этом проверяются две альтернативы:

в описании могут быть указаны признаки, сочетание которых практически наверняка достаточно для справедливости определенной фразы из заключения, но врачом эта фраза не указана; может быть такой вариант заключения, для которого в описании не указан ни один из необходимых для этого признаков.

Интеллектуальное АРМ, содержимое БЗ которого отвечает всем принципам [верификации](http://pandia.ru/text/category/verifikatciya/) в конкретной предметной области, обеспечивает более высокое качество предлагаемых врачу-пользователю решений.

Специализированные рабочие места

Понятие «типовое АРМ» базируется на общих принципах его построения и функционирования. Это необходимое условие для разработки совместимых АРМ. Такой подход не исключает, однако, того, что в реальности большинство АРМ имеет особенности, обусловленные их профилем, которые реализуются в виде определенного набора функций. Рассмотрим примеры АРМ различного профиля.

Для АРМ врача в операционных (рабочее место [анестезиолога](http://www.pandia.ru/text/category/anesteziologiya/)) и последующего наблюдения в палатах интенсивной терапии (рабочее место реаниматолога) важной частью является система сбора, хранения и представления мониторируемых непрерывно (ЭКГ, артериального давления и т. п.) и дискретно (неинвазивного артериального давления, сердечного выброса и т. п.) параметров, а также данных с устройств, например, с автоматических капелниц (скорость, время подачи лекарств и т. п.), аппарата искусственного дыхания (газовый состав, объем вдыхаемой смеси и т. п.), аппарата искусственного кровообращения (расход крови, температура и т. п.).

Автоматизированное рабочее место врача-хирурга должно включать конструктор протоколов операций на основе типовых шаблонов в соответствии с профилем отделения, что ускоряет работу врача и предотвращает пропуск необходимых записей.

Автоматизированное рабочее место врача-эндоскописта обеспечивает привязку описания к технологии обследования и включает диагностические описания, сопровождаемые [видеозаписями](http://www.pandia.ru/text/category/videozapismz/) наблюдаемой у больного картины и произведенных манипуляций.

Автоматизированное рабочее место клинического фармаколога поддерживает следующие функции:

ведение фармакологического справочника; ведение стандартных схем лечения; анализ взаимодействия лекарственных средств; анализ и профилактика побочных эффектов лекарственных веществ; разработка индивидуальных схем лечения; формирование, анализ и корректировка назначений с учетом подбора оптимальных для конкретного больного препаратов среди медикаментов-аналогов.

Автоматизированное рабочее место руководителя МО предполагает доступ к электронным записям о пациентах, статистической, финансовой и хозяйственной информации, а также предоставляет современные средства обмена данными.

Автоматизированное рабочее место главного специалиста той или иной службы региона позволяет анализировать деятельность службы в целом и ее структурных подразделений в разрезе районов и городов территории.

Автоматизированное рабочее место организатора здравоохранения должно обеспечивать поддержку текущих и перспективных решений, включая прогнозирование уровня заболеваемости населения в разных ситуациях и при различном уровне экологического загрязнения района проживания, экономические аспекты деятельности.

Электронная история болезни

Электронная история болезни (ЭИБ) - это составляющая информационной системы, обеспечивающая автоматизацию ведения и формирования медицинской документации, оперативный обмен между участниками лечебно-диагностического процесса (ЛДП) и поддержку их деятельности.

Концептуальная основа компьютеризированной или электронной истории болезни заключается в следующих принципах:

единство информации о пациенте, предполагающее однократный [ввод данных](http://pandia.ru/text/category/vvod_dannih/) в систему; доступность информации о больных для просмотра всеми участниками ЛДП в любой момент времени в любом месте (с учетом ограничений по принципам конфиденциальности на основе санкционированных прав доступа) при одновременной защищенности от внесения изменений; единые классификаторы (периодически обновляемые); автоматическое вычисление производных показателей (длительность госпитализации, количество дней до и после операции, опасность инфекционных осложнений, наличие шока, необходимый объем инфузионной терапии и др.) после введения первичной информации; технологически функциональное включение СППР; диспетчеризация (управление) в вопросах обследования пациентов.

Концепция ЭИБ определяет соответствующую технологию их построения, включающую следующее:

модульный принцип, обеспечивающий возможность наращивания и модификации системы без ее перестройки в целом, что избавляет пользователей от необходимости ее повторного освоения; создание компьютерной сети сложной топологии, т. е. включающей иерархию локальных сетей подразделений в многопрофильных больницах; включение ранее созданного прикладного математического обеспечения медицинского назначения для решения различных задач (например, расчет специальных диет); подключение АРМ и аппаратно-программных комплексов; открытые для пополнения врачами-пользователями классификаторы клинических записей (при условии модификации и пополнения общих классификаторов нормативно-справочной информации только администратором БД по указанию главного врача или его заместителя по лечебной работе); автоматическое формирование медицинских документов и заявок на исследования на основе ранее введенных данных; автоматическое направление результатов исследований и осмотров больных консультантами в соответствующие лечебные подразделения; автоматическое формирование листа назначений (для медицинской сестры) на основе врачебных записей; ведение листа назначений (отметок о выполнении) медицинской сестрой.

Ядром [базы данных](http://www.pandia.ru/text/category/bazi_dannih/) ЭИБ является «запись пациента», представляющая собой электронный аналог истории болезни.

Функции и общие принципы построения ЭИБ многопрофильного стационара едины для всех учреждений, в то время как ее структура и методы реализации определяются особенностями конкретной больницы и техническими возможностями (особенностями) построения.

Главной задачей ЭИБ является документирование ЛДП в сочетании с управлением этим процессом.

Рассмотрим некоторые преимущества электронных карт перед рукописными:

удобочитаемость  и точность (по сравнению с рукописными); могут включать различные виды информации (результаты исследований в виде звуковых файлов, видео - файлов, графических файлов); сокращение времени на оформление документов за счет уменьшения набора текста при использовании шаблонов, выбора из предложенного списка, автозаполнения; быстрый доступ (уменьшается время доступа; доступ не локальный, а глобальный: сколь угодно большое число медработников одновременно могут использовать информацию); оптимизация поиска необходимой информации (по фамилии, дате, диагнозу и т. д.); возможность напоминания и сигналов; оптимизация хранения информации; поддержка статистических отчетов и научных исследований (быстро осуществляются выборки данных, генерируются отчеты в автоматическом режиме); защита данных (разрешение/запрет просмотра и редактирования данных); конфиденциальность информации (возможность организации ограниченного доступа к карте по системе паролей); информация может быть в любой момент распечатана на принтере любом количестве экземпляров.

Электронная история болезни – это не столько автоматизация ведения медицинских записей, сколько [новая технология](http://www.pandia.ru/text/category/novie_tehnologii/), освобождающая медицинский персонал от значительной части действий, не требующих осмысления, и обеспечивающая представление первично обработанной информации, а также создание новых условий для взаимодействия различных подразделений МО.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

С какой целью производится автоматизация рабочего места сотрудника? Перечислите общие принципы создания АРМ врача. Какие требования предъявляются к АРМ врача. Приведите примеры сотрудников МО, нуждающихся в создании АРМ. Что собой представляет АРМ медицинского работника? В чем заключаются особенности интеллектуального АРМ? Назовите основные функции АРМ врача. По каким принципам классифицируются медицинские АРМ? Что означает понятие «типовое АРМ»? Дайте характеристику специализированным АРМ. Каковы функции АРМ клинического фармаколога? Каковы функции АРМ организатора здравоохранения? Что такое электронная история болезни? Назовите концептуальную  основу электронной истории болезни? Какова технология построения электронной истории болезни? Назовите преимущества электронных карт амбулаторных и стационарных больных перед рукописными.

ТЕМА №7

Информационная безопасность. Право доступа к  информации и конфиденциальность медицинских данных.

Необходимо знать: виды регламентируемой информации, носители информации; понятия государственной тайны, конфиденциальной информации, понятия [защиты информации](http://pandia.ru/text/category/zashita_informatcii/), угрозы, атаки, окна опасности,  основные угрозы информации,  уровни защиты информации,  этапы  создания системы защиты информации; понятие компьютерного [вируса](http://www.pandia.ru/text/category/virus/), антивирусных программ, санкционированного доступа,  аутентификации пользователей, электронно-цифровой подписи, персональных данных пациента.

Необходимо уметь: использовать антивирусное программное обеспечение.

Медицинские данные на любом уровне представляют собой ценный стратегический ресурс, доступ к которому необходимо строго контролировать, регламентировать, обеспечивая безопасное хранение данных.

Широкое использование информации в системе здравоохранения ставит перед ней новые проблемы — обеспечение информационной защиты используемых персонифицированных данных, касающихся здоровья или относящихся к разряду конфиденциальных.

По характеру ограничений конституционных прав и свобод в ин-формационной сфере выделяют четыре основных вида правовой (регламен-тированной законами) информации:

- информация с ограниченным доступом;

- информация без права ограничения;

- иная общедоступная информация;

- «вредная» информация (информация, не подлежащая распространению как недостоверная, ложная и т. п.).

Информация с ограниченным доступом делится на государственную тайну и конфиденциальную.

К государственной тайне относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.

Владельцем государственной тайны является само государство. Требования по защите этой информации и контроль за их соблюдением регламентируются Законом РФ «О государственной тайне».  В нем законодательно установлен Перечень сведений, сопоставляющих государственную тайну, и круг сведений, не подлежащих к отнесению к ней.

Конфиденциальная информация – это документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности.

Этой информацией владеют различные учреждения, организации и отдельные индивидуумы. Конфиденциальная информация делится на шесть видов:

- тайна следствия и судопроизводства;

- служебная тайна;

- профессиональная тайна;

- [коммерческая тайна](http://pandia.ru/text/category/kommercheskaya_tajna/);

- сведения о сущности изобретения, полезной модели или промышленного образца по официальной публикации информации о них;

- персональные данные.

Основными носителями информации являются:

- открытая печать (газеты, журналы, отчеты, реклама и т. д.);

- люди;

- средства связи (радио, телевидение, телефон, пейджер и т. д.);

- документы (официальные, деловые, личные и т. д.);

- электронные, магнитные и другие носители, пригодные для автоматической обработки данных.

Интенсивное развитие компьютерных средств и [информационных технологий](http://pandia.ru/text/category/informatcionnie_tehnologii/) повышают требования к обеспечению [информационной безопасности](http://www.pandia.ru/text/category/informatcionnaya_bezopasnostmz/).

Информационная безопасность - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе [владельцам](http://www.pandia.ru/text/category/vladeletc/) и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение [информационной безопасности](http://pandia.ru/text/category/bezopasnostmz_informatcionnaya/).

Защита информации должна быть основана на системном подходе. Системный подход заключается в том, что все средства, используемые для обеспечения информационной безопасности должны рассматриваться как единый комплекс взаимосвязанных мер.

Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, - злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

[](https://yandex.ru/an/count/X2uejI_zO0a49I40z3W8dMn1aUAxS0K02GKnzIvHOW00000uffiVXfFitvZMxPkV0O010OW1-9INX841a06wkeJcs820W0AO0RgwXEPOe06ikQW1hBc4vbYu0UYzfA0Zm042s07qafEV0U01Wh-u7UW1r0C9c0Ag-laNe0B0ie4JkG91LhDvieme_y022_02bz-fhm70iRK2-0Ighy0BY0MxYEK7a0Mghy0Be0MbcS43g0MqglO2i0MqglO2k0MqglO2m0MjulyBo0N6kOO3q0NVtPK1u0MLaioMemUW1eAi0QW6Wgm1oGPvz5zYtnAQHAa7EiqeCcrFx1Yu1u05q0SMs0SG2iA2W0RW2A3Pm0de2GTnq3HRPKplFyaIgWiGoZ73uZhD003Foj12Czpe2zlNeW7m2mk83EoR1fWDk8c1W82023_vwF-Izjk4pKIW3i24FRgQizlJxPFs680GkeVo7v0GqC-XiQwhc-zamA0Qq12CegzV-10FW14IPx2aeiC9u16d-FO5w173kSV1ZRlEeubIga2cGk3dNM_pF-aIrIy0ncXHTReoc1C4g1EI_-UekhhkuHRW4ydCymA05810Y1IejUxVniQCqgy1e1J9pFC2g1IepxKBm1I0sis33TWKcwI_aWRW507e58m2q1MRfB-I1jWLmOhsxAEFlFnZyA0Mu9w_aWQm5h83oHRG5kpfthu1s1Q15vWN_vVv8gWN2RWN0S0NjHRG5z260zWNyUaxu1U4dT3r1UWN0VWNzFZ7aGQP6A0O5R0OYB_4aWQu607G627u6FQJg-gNoekDwW606R3qkEBGlP6v88aPo_W70A0PWgm1i1cu6S3I6H9vOM9pNtDbSdPbSYzoDZKnBJFW6G7e6O320_0PWC83WHh__qzs3BBjt8WQm8Gzc1hKmrEW6i_ifhJamzQZY06m6lBLfkNjaSp8i06u6WBr6W40002O6xY9Eh0RFBWR0zWRW07f6m000E03Mb91y1lkze89WXmDJpL1Ecj4KZbQEKzPDzWSrR-X0U0SgC-r2-aSyHm0001WzmD-Fu0T_t-P7U0TeS85w1s0qEJlbhsd-YBm7VdqvRclYkViAlWTlfgjhxoQbzKYYHxulsPBvH7lFv4Ug1u1q1x4_E3ml_oZoFW1s1xwsXw87____m6W7xg7yX-m7m787xh9oK_I7mKrDpKoC_WV0O0W0eWW0QaWi224W23O8F__0U0W0IqWSOH68OUSWixKr0wSsVWQUSWOJIGZK2WXFfaJvNv4T9j1U3Tdgjq8fLY9Vf2MGKN6IEJBiXz6GeOIPi6hNGabjl5973j9vBQLQ6TszIDgSYN1wcDO_bTSawyffsZ2QnybQof7weK0M0yzWfTi2r4v-YcHts11OUdJAldu86_kWxdXJuizo22QPb65h33hg6qB7W00~1?stat-id=9&test-tag=98457830349329&banner-sizes=eyI3MjA1NzYwNTk1NjA3OTI2MSI6IjMzNHgyNzgifQ%3D%3D&format-type=118&actual-format=13&pcodever=57523&banner-test-tags=eyI3MjA1NzYwNTk1NjA3OTI2MSI6IjQyOTUwMTY0NjUifQ%3D%3D&pcode-active-testids=560593%2C0%2C1%3B555795%2C0%2C52&width=336&height=280" \t "_blank)

[](https://yandex.ru/an/count/X2uejI_zO0a49I40z3W8dMn1aUAxS0K02GKnzIvHOW00000uffiVXfFitvZMxPkV0O010OW1-9INX841a06wkeJcs820W0AO0RgwXEPOe06ikQW1hBc4vbYu0UYzfA0Zm042s07qafEV0U01Wh-u7UW1r0C9c0Ag-laNe0B0ie4JkG91LhDvieme_y022_02bz-fhm70iRK2-0Ighy0BY0MxYEK7a0Mghy0Be0MbcS43g0MqglO2i0MqglO2k0MqglO2m0MjulyBo0N6kOO3q0NVtPK1u0MLaioMemUW1eAi0QW6Wgm1oGPvz5zYtnAQHAa7EiqeCcrFx1Yu1u05q0SMs0SG2iA2W0RW2A3Pm0de2GTnq3HRPKplFyaIgWiGoZ73uZhD003Foj12Czpe2zlNeW7m2mk83EoR1fWDk8c1W82023_vwF-Izjk4pKIW3i24FRgQizlJxPFs680GkeVo7v0GqC-XiQwhc-zamA0Qq12CegzV-10FW14IPx2aeiC9u16d-FO5w173kSV1ZRlEeubIga2cGk3dNM_pF-aIrIy0ncXHTReoc1C4g1EI_-UekhhkuHRW4ydCymA05810Y1IejUxVniQCqgy1e1J9pFC2g1IepxKBm1I0sis33TWKcwI_aWRW507e58m2q1MRfB-I1jWLmOhsxAEFlFnZyA0Mu9w_aWQm5h83oHRG5kpfthu1s1Q15vWN_vVv8gWN2RWN0S0NjHRG5z260zWNyUaxu1U4dT3r1UWN0VWNzFZ7aGQP6A0O5R0OYB_4aWQu607G627u6FQJg-gNoekDwW606R3qkEBGlP6v88aPo_W70A0PWgm1i1cu6S3I6H9vOM9pNtDbSdPbSYzoDZKnBJFW6G7e6O320_0PWC83WHh__qzs3BBjt8WQm8Gzc1hKmrEW6i_ifhJamzQZY06m6lBLfkNjaSp8i06u6WBr6W40002O6xY9Eh0RFBWR0zWRW07f6m000E03Mb91y1lkze89WXmDJpL1Ecj4KZbQEKzPDzWSrR-X0U0SgC-r2-aSyHm0001WzmD-Fu0T_t-P7U0TeS85w1s0qEJlbhsd-YBm7VdqvRclYkViAlWTlfgjhxoQbzKYYHxulsPBvH7lFv4Ug1u1q1x4_E3ml_oZoFW1s1xwsXw87____m6W7xg7yX-m7m787xh9oK_I7mKrDpKoC_WV0O0W0eWW0QaWi224W23O8F__0U0W0IqWSOH68OUSWixKr0wSsVWQUSWOJIGZK2WXFfaJvNv4T9j1U3Tdgjq8fLY9Vf2MGKN6IEJBiXz6GeOIPi6hNGabjl5973j9vBQLQ6TszIDgSYN1wcDO_bTSawyffsZ2QnybQof7weK0M0yzWfTi2r4v-YcHts11OUdJAldu86_kWxdXJuizo22QPb65h33hg6qB7W00~1?stat-id=9&test-tag=98457830349329&banner-sizes=eyI3MjA1NzYwNTk1NjA3OTI2MSI6IjMzNHgyNzgifQ%3D%3D&format-type=118&actual-format=13&pcodever=57523&banner-test-tags=eyI3MjA1NzYwNTk1NjA3OTI2MSI6IjQyOTUwMTY0NjUifQ%3D%3D&pcode-active-testids=560593%2C0%2C1%3B555795%2C0%2C52&width=336&height=280" \t "_blank)

[reg.rrost.ru](https://yandex.ru/an/count/X2uejI_zO0a49I40z3W8dMn1aUAxS0K02GKnzIvHOW00000uffiVXfFitvZMxPkV0O010OW1-9INX841a06wkeJcs820W0AO0RgwXEPOe06ikQW1hBc4vbYu0UYzfA0Zm042s07qafEV0U01Wh-u7UW1r0C9c0Ag-laNe0B0ie4JkG91LhDvieme_y022_02bz-fhm70iRK2-0Ighy0BY0MxYEK7a0Mghy0Be0MbcS43g0MqglO2i0MqglO2k0MqglO2m0MjulyBo0N6kOO3q0NVtPK1u0MLaioMemUW1eAi0QW6Wgm1oGPvz5zYtnAQHAa7EiqeCcrFx1Yu1u05q0SMs0SG2iA2W0RW2A3Pm0de2GTnq3HRPKplFyaIgWiGoZ73uZhD003Foj12Czpe2zlNeW7m2mk83EoR1fWDk8c1W82023_vwF-Izjk4pKIW3i24FRgQizlJxPFs680GkeVo7v0GqC-XiQwhc-zamA0Qq12CegzV-10FW14IPx2aeiC9u16d-FO5w173kSV1ZRlEeubIga2cGk3dNM_pF-aIrIy0ncXHTReoc1C4g1EI_-UekhhkuHRW4ydCymA05810Y1IejUxVniQCqgy1e1J9pFC2g1IepxKBm1I0sis33TWKcwI_aWRW507e58m2q1MRfB-I1jWLmOhsxAEFlFnZyA0Mu9w_aWQm5h83oHRG5kpfthu1s1Q15vWN_vVv8gWN2RWN0S0NjHRG5z260zWNyUaxu1U4dT3r1UWN0VWNzFZ7aGQP6A0O5R0OYB_4aWQu607G627u6FQJg-gNoekDwW606R3qkEBGlP6v88aPo_W70A0PWgm1i1cu6S3I6H9vOM9pNtDbSdPbSYzoDZKnBJFW6G7e6O320_0PWC83WHh__qzs3BBjt8WQm8Gzc1hKmrEW6i_ifhJamzQZY06m6lBLfkNjaSp8i06u6WBr6W40002O6xY9Eh0RFBWR0zWRW07f6m000E03Mb91y1lkze89WXmDJpL1Ecj4KZbQEKzPDzWSrR-X0U0SgC-r2-aSyHm0001WzmD-Fu0T_t-P7U0TeS85w1s0qEJlbhsd-YBm7VdqvRclYkViAlWTlfgjhxoQbzKYYHxulsPBvH7lFv4Ug1u1q1x4_E3ml_oZoFW1s1xwsXw87____m6W7xg7yX-m7m787xh9oK_I7mKrDpKoC_WV0O0W0eWW0QaWi224W23O8F__0U0W0IqWSOH68OUSWixKr0wSsVWQUSWOJIGZK2WXFfaJvNv4T9j1U3Tdgjq8fLY9Vf2MGKN6IEJBiXz6GeOIPi6hNGabjl5973j9vBQLQ6TszIDgSYN1wcDO_bTSawyffsZ2QnybQof7weK0M0yzWfTi2r4v-YcHts11OUdJAldu86_kWxdXJuizo22QPb65h33hg6qB7W00~1?stat-id=9&test-tag=98457830349329&banner-sizes=eyI3MjA1NzYwNTk1NjA3OTI2MSI6IjMzNHgyNzgifQ%3D%3D&format-type=118&actual-format=13&pcodever=57523&banner-test-tags=eyI3MjA1NzYwNTk1NjA3OTI2MSI6IjQyOTUwMTY0NjUifQ%3D%3D&pcode-active-testids=560593%2C0%2C1%3B555795%2C0%2C52&width=336&height=280" \t "_blank)

РЕКЛАМА

[**Выпуск акций от 6 дней. Скидка 40% для новых клиентов!**](https://yandex.ru/an/count/X2uejI_zO0a49I40z3W8dMn1aUAxS0K02GKnzIvHOW00000uffiVXfFitvZMxPkV0O010OW1-9INX841a06wkeJcs820W0AO0RgwXEPOe06ikQW1hBc4vbYu0UYzfA0Zm042s07qafEV0U01Wh-u7UW1r0C9c0Ag-laNe0B0ie4JkG91LhDvieme_y022_02bz-fhm70iRK2-0Ighy0BY0MxYEK7a0Mghy0Be0MbcS43g0MqglO2i0MqglO2k0MqglO2m0MjulyBo0N6kOO3q0NVtPK1u0MLaioMemUW1eAi0QW6Wgm1oGPvz5zYtnAQHAa7EiqeCcrFx1Yu1u05q0SMs0SG2iA2W0RW2A3Pm0de2GTnq3HRPKplFyaIgWiGoZ73uZhD003Foj12Czpe2zlNeW7m2mk83EoR1fWDk8c1W82023_vwF-Izjk4pKIW3i24FRgQizlJxPFs680GkeVo7v0GqC-XiQwhc-zamA0Qq12CegzV-10FW14IPx2aeiC9u16d-FO5w173kSV1ZRlEeubIga2cGk3dNM_pF-aIrIy0ncXHTReoc1C4g1EI_-UekhhkuHRW4ydCymA05810Y1IejUxVniQCqgy1e1J9pFC2g1IepxKBm1I0sis33TWKcwI_aWRW507e58m2q1MRfB-I1jWLmOhsxAEFlFnZyA0Mu9w_aWQm5h83oHRG5kpfthu1s1Q15vWN_vVv8gWN2RWN0S0NjHRG5z260zWNyUaxu1U4dT3r1UWN0VWNzFZ7aGQP6A0O5R0OYB_4aWQu607G627u6FQJg-gNoekDwW606R3qkEBGlP6v88aPo_W70A0PWgm1i1cu6S3I6H9vOM9pNtDbSdPbSYzoDZKnBJFW6G7e6O320_0PWC83WHh__qzs3BBjt8WQm8Gzc1hKmrEW6i_ifhJamzQZY06m6lBLfkNjaSp8i06u6WBr6W40002O6xY9Eh0RFBWR0zWRW07f6m000E03Mb91y1lkze89WXmDJpL1Ecj4KZbQEKzPDzWSrR-X0U0SgC-r2-aSyHm0001WzmD-Fu0T_t-P7U0TeS85w1s0qEJlbhsd-YBm7VdqvRclYkViAlWTlfgjhxoQbzKYYHxulsPBvH7lFv4Ug1u1q1x4_E3ml_oZoFW1s1xwsXw87____m6W7xg7yX-m7m787xh9oK_I7mKrDpKoC_WV0O0W0eWW0QaWi224W23O8F__0U0W0IqWSOH68OUSWixKr0wSsVWQUSWOJIGZK2WXFfaJvNv4T9j1U3Tdgjq8fLY9Vf2MGKN6IEJBiXz6GeOIPi6hNGabjl5973j9vBQLQ6TszIDgSYN1wcDO_bTSawyffsZ2QnybQof7weK0M0yzWfTi2r4v-YcHts11OUdJAldu86_kWxdXJuizo22QPb65h33hg6qB7W00~1?stat-id=9&test-tag=98457830349329&banner-sizes=eyI3MjA1NzYwNTk1NjA3OTI2MSI6IjMzNHgyNzgifQ%3D%3D&format-type=118&actual-format=13&pcodever=57523&banner-test-tags=eyI3MjA1NzYwNTk1NjA3OTI2MSI6IjQyOTUwMTY0NjUifQ%3D%3D&pcode-active-testids=560593%2C0%2C1%3B555795%2C0%2C52&width=336&height=280)

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Различают следующие виды угроз информации:

•        уничтожение (может быть уничтожена как сама информация, так и ее носитель);

•        несанкционированное получение и распространение конфиденциальной информации (это наиболее часто встречающийся вид угроз);

•        несанкционированная модификация информации;

•        создание ложных сообщений;

•        блокирование доступа к информации;

•        несанкционированное или ошибочное использование информационных ресурсов системы;

•        отказ в получении или отправке информации.

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход. Выделяют следующие уровни защиты информации:

законодательный – законы, [нормативные акты](http://pandia.ru/text/category/akt_normativnij/) и прочие документы РФ и международного сообщества; административный – комплекс мер, предпринимаемых локально руководством организации; процедурный уровень – меры безопасности, реализуемые людьми; программно-технический уровень – непосредственно средства защиты информации.

Применительно к информационным системам процесс создания системы защиты информации подразумевает прохождение ряда этапов:

•        выявление угроз защищаемой информации;

•        определение политики безопасности - свода правил обращения с конфиденциальной информацией;

•        создание механизмов поддержки политики безопасности (средства идентификации пользователей и контроля доступа, шифрования информации, электронно-цифровой подписи, антивирусные средства и т. д.);

•        оценка защищенности системы.

Массовое использование компьютеров, а также быстрое развитие компьютерных сетей (в частности сети Интернет) способствовали появлению и распространению вредоносных программ – компьютерных вирусов. Вирусы порой делают работу на компьютере невозможной. Они могут нанести значительный ущерб, как информации, так и самому компьютеру.

Компьютерный вирус – это программа, которая способна самостоятельно создавать свои копии и внедряться в другие программы и системные области дисковой памяти компьютера либо распространяться по каналам связи.

Свое название компьютерный вирус получил за некоторое сходство с биологическим вирусом. Например, в зараженной программе самовоспроизводится вирус, а инфицированная программа может длительное время работать без ошибок, как в стадии инкубации, а потом при определенных условиях начать заражать другие компьютеры.

Важное свойство компьютерных вирусов – способность «размножаться» (создавать свои копии), бесконтрольно распространяясь на компьютере или даже на всех компьютерах в сети. Основной целью программ-вирусов является нарушение работы ОС и прикладных программ, порча файловых систем и компонентов компьютера, дестабилизация работы пользователей или серверов интернет сайтов. Программа, внутри которой находится вирус, называется зараженной (инфицированной).

Одним из видов вредоносных программ являются «сетевые черви» – вредоносные программы, которые распространяются по компьютерным сетям, вычисляя адреса сетевых компьютеров и рассылая по этим адресам свои копии. Также существуют  троянские программы  – вредоносные программы, которые не способны к самораспространению, а маскируются под какую-то полезную или интересную программу, разрушают загрузочный сектор и файловую систему или собирают и пересылают своему создателю информацию, не подлежащую разглашению (например, ваши личные пароли).

Для защиты компьютеров от большинства вирусов, червей и «троянских коней», которые могут удалять файлы, получать доступ к личным данным или использовать зараженную систему как средство атаки на другие компьютеры существуют антивирусные программы.

Антивирусная программа (антивирус) – программа для обнаружения компьютерных вирусов и других вредоносных программ, лечения и восстановления инфицированных файлов, а также для профилактики – предотвращения заражения вредоносным кодом.

Антивирусные программы обычно используют два различных метода:

1) сканирование (просмотр) файлов для поиска уже известных вирусов.

2) обнаружение подозрительного поведения любой программы («эвристическое сканирование»).

Рассмотрим вопрос  о праве доступа к  медицинской информации  и конфиденциальность медицинских данных.

К медицинской информации в силу своей деятельности имеют доступ многочисленные пользователи:  врачи, средние медицинские работники, руководители здравоохранения различного уровня. И это создает проблемы в отношении конфиденциальности персональных данных пациентов. Решение состоит в предоставлении каждому из обращающихся к информационно-технологической системе (ИТС) соответствующих прав (уровней доступа) ко всей базе данных или отдельным ее разделам, т. е. прав на ознакомление с различными данными пациентов и осуществление различных действий. Этот подход носит название санкционированного многоуровневого доступа.

Полный доступ к данным конкретного больного имеют лечащий врач, заведующий отделением и другие медицинские руководители, по роду своей деятельности контактирующие с больными и(или) обладающие правами контроля деятельности лечащих врачей. Для врачей-специалистов, обеспечивающих консультативную помощь и проводящих исследования, могут быть введены определенные ограничения на просмотр информации о пациенте.

Решение вопроса защиты данных обеспечивается путем идентификации каждого из медицинских работников и проверки подлинности, то есть аутентификации пользователей.

Таким путем осуществляется ограничение доступа к данным с учетом должностных или функциональных обязанностей. Особенно жесткие требования предъявляются в отношении разрешения на коррекцию информации. Изменения в персональных данных после завершения дневной работы или запрещаются, или разрешаются при одновременном сохранении в базе данных сделанных ранее записей, кото­рые могут быть доступны для просмотра при использовании определенного режима работы (механизм подотчетности, т. е. протоколирование действий). Так обеспечивается конфиденциальность, т. е. защита от несанкционированного получения информации, и целостность - защита от несанкционированного изменения информации.

Технически вопрос конфиденциальности и защиты данных обеспечивается использованием иерархической системы паролей, присваиваемых пользователям и определяющих их право на просмотр и (или) внесение новых записей. Пользователи оперируют данными, хранящимися в базе данных, в рамках выделенных им привилегий, которые определяют права их доступа к определенной информации.

Систему паролей можно представить следующим образом:

пароль на вход в информационную [медицинскую систему](http://www.pandia.ru/text/category/meditcinskoe_oborudovanie/); пароли на определенные роли (права) пользователей (например, ввод, корректировку, просмотр персональных данных), в отношении которых проводится проверка ФИО с последующим подтверждением должности или временных функций (например, дежурный врач); пароли на модули системы (например, на просмотр и (или) корректировку родословной).

Такими способами может быть реализован ограниченный доступ к медицинским базам данных, сочетающий проверку прав на определенные действия с проверкой прав на доступ к определенным разделам баз данных. Таким путем обеспечиваются конфиденциальность и защита данных пациентов при условии аутентификации и [авторизации](http://pandia.ru/text/category/avtorizatciya/) пользователей, в том числе и сотрудников [вычислительных центров](http://www.pandia.ru/text/category/informatcionno_vichislitelmznie_tcentri/), обеспечивающих работу с ИТС.

Использование электронной цифровой подписи позволяет установить автора электронного документа и гарантировать неизменность его содержания. Это специфический «цифровой код», интегрированный с содержанием электронного документа и позволяющий идентифицировать его отправителя (автора), а также установить отсутствие искажений информации в электронном документе, поскольку в случае внесения в него изменений электронная цифровая подпись теряет силу.

В соответствии с Федеральным законом от 01.01.01 г. «Об информации, информационных технологиях и о защите информации» электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью. Применение электронной цифровой подписи в соответствии с требованиями Федеральных законов от 01.01.01 г. «Об электронной цифровой подписи» и «Об информации, информационных технологиях и о защите информации» является одним из условий организации юридически значимого обмена электронными документами. В настоящее время в российском здравоохранении осуществляется внедрение цифровой подписи.

Каждая ме­дицинская организация, являясь оператором персональных данных, обязана обеспечить на­дежную защиту получаемых в ее распоряжение данных о пациенте. Персональные данные, обрабатываемые в медицине, должны быть за­щищены на очень высоком уровне защиты, что обеспечивается путем создания специаль­ной системы персональных данных.

Закон «О персональных данных» делит персональные данные на три категории:

• общедоступные – основные анкетные дан­ные (имя, отчество, фамилия, гендерная принадлежность, дата рождения и т. д.);

• биометрические – внешние данные и не­которые физиологические особенности (последние – при условии их визуального определения);

• специальные – национальность, вероиспо­ведание, сведения о состоянии здоровья, а также данные о [взаимоотношениях](http://www.pandia.ru/text/category/vzaimootnoshenie/) с зако­ном (судимость, привлечение к ответствен­ности), частично – информация в сфере за­нятости (причины увольнения и т. д.).

       Обработка персональных дан­ных – это любое действие (операция) или совокупность действий (операций), совершае­мых с использованием средств автоматизации или без использования таких средств с персо­нальными данными, включая:

• сбор, запись, систематизацию, накопление;

• хранение, уточнение (обновление, измене­ние), извлечение;

• использование, передачу (распространение, предоставление, доступ), обезличивание;

• блокирование, удаление, уничтожение пер­сональных данных.

По общему правилу обработка персональ­ных данных возможна с согласия субъекта персональных данных (п. 1 ч. 1 ст. 6, п. 1 ч. 2 ст. 10 Федерального закона N 152–ФЗ).

В силу ч. 4 ст. 9 Федерального закона N 152-ФЗ согласие субъекта персональных данных на обработку его персональных данных, состав­ленное в письменной форме, должно вклю­чать, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведе­ния о дате выдачи указанного документа и вы­давшем его органе;

2) фамилию, имя, отчество, адрес предста­вителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указан­ного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого предста­вителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отче­ство и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обра­ботку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отче­ство и адрес лица, осуществляющего обработку персональных данных по поручению операто­ра, если обработка будет поручена такому лицу;

7) перечень действий с персональными дан­ными, на совершение которых дается согласие, общее описание используемых оператором спо­собов обработки персональных данных;

8) срок, в течение которого действует со­гласие субъекта персональных данных, а так­же способ его отзыва, если иное не установле­но федеральным законом;

9) подпись субъекта персональных данных.

Важно правильно соотносить понятия «персональные данные» и «врачебная тайна». Врачебная тайна представляет собой сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здо­ровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении. Соблюдение врачебной тайны является од­ним из принципов охраны здоровья (статья 4 Закона об основах охраны здоровья граж­дан). Врачебная тайна является особым режимом информации с ограниченным доступом. Если сравнивать понятия «персональные дан­ные» и «врачебная тайна», то последнее явля­ется более узким понятием. Врачебная тайна выступает видом персональных данных, кото­рый становится известным медицинской ор­ганизации при оказании медицинских услуг. Однако пациент имеет право на защиту лю­бой информации о нем, которая стала извест­на медицинской организации. Закон об осно­вах охраны здоровья разрешает медицинской организации разглашать другим лицам сведе­ния, составляющие врачебную тайну или иные персональные данные пациента только с пись­менного согласия пациента либо его законного представителя.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

Какие виды регламентируемой информации принято выделять? Что такое государственная тайна? Что такое конфиденциальная информация? Приведите примеры носителей информации. Дайте определение информационной безопасности. Что такое защита информации? Дайте определение информационной угрозе. Расскажите об информационной атаке, источнике угрозы. Что понимают под термином «окно опасности»? Перечислите известные вам виды угроз информации. Какие выделяют уровни защиты информации? Перечислите этапы  создания системы защиты информационной системы. Что такое компьютерный вирус? Как осуществляется антивирусная защита компьютера? Какие медицинские данные требуют защиты? Что означает санкционированный доступ? Что такое аутентификации пользователей? Как организуется система паролей для обеспечения конфиденциальности данных? Что такое электронно-цифровая подпись? Расскажите о правилах обработки персональных данных в МО? Что такое согласие пациента на обработку персональных данных?