**Лекция 4**

**Обеспечение информационной безопасности при работе с медицинскими данными**

**Цель занятия:** получить знания о конфиденциальной информации и способах обеспечения её защиты в медицинских организациях.

Медицинские данные на любом уровне представляют собой ценный стратегический ресурс, доступ к которому необходимо строго контролировать, регламентировать, обеспечивая безопасное хранение данных. Информация, обрабатываемая и используемая в медицинских организациях, относится к категории конфиденциальной.

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

С точки зрения конфиденциальности информации **в МО используются:**

1. персональные данные, составляющие "личную тайну", а также врачебную тайну;
2. технико-экономические данные (о взаиморасчетах между учреждениями здравоохранения), составляющие коммерческую тайну;
3. данные о медико-демографической и эпидемиологической ситуации, составляющие служебную тайну.

В медицинских организациях обрабатываются различные виды и категории персональных данных пациентов. Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» определяет, что при ведении персонифицированного учета сведений о застрахованных лицах осуществляются сбор, обработка, передача и хранение следующих сведений о застрахованных лицах:

1) фамилия, имя, отчество;
2) пол;
3) дата рождения;
4) место рождения;
5) гражданство;
6) данные документа, удостоверяющего личность;
7) место жительства;
8) место регистрации;
9) дата регистрации;
10 страховой номер индивидуального лицевого счета (СНИЛС);
11 номер полиса обязательного медицинского страхования застрахованного лица;
12 данные о страховой медицинской организации, выбранной застрахованным лицом;
13 дата регистрации в качестве застрахованного лица;
14 статус застрахованного лица (работающий, неработающий);
15 сведения о медицинской организации, выбранной застрахованным лицом в соответствии с законодательством Российской Федерации для получения первичной медико-санитарной помощи.

В этом же законе определено, что при ведении персонифицированного учета сведений о медицинской помощи, оказанной застрахованным лицам, осуществляются сбор, обработка, передача и хранение следующих сведений:

- номер полиса обязательного медицинского страхования застрахованного лица;
- сведения о медицинской организации, оказавшей медицинские услуги;
- виды оказанной медицинской помощи;
- условия оказания медицинской помощи;
- формы оказания медицинской помощи;
- сроки оказания медицинской помощи;
- объемы оказанной медицинской помощи;
- стоимость оказанной медицинской помощи;
- диагноз;
- профиль оказания медицинской помощи;

- сведения о медицинских услугах, оказанных застрахованному лицу, и о примененных лекарственных препаратах;
- примененные стандарты оказания медицинской помощи;
- сведения о медицинском работнике или медицинских работниках, оказавших медицинские услуги;
- результат обращения за медицинской помощью;
- результаты проведенного контроля объемов, сроков, качества и условий предоставления медицинской помощи.

Кроме этого в отдельных случаях в МО могут собираться и другие сведения, необходимые для оказания медицинских услуг и их учета, например:

- семейное положение;
- социальное положение;
- сведения об образовании, профессии;
- сведения о состоянии здоровья;
- личная фотография;
- идентификационный номер налогоплательщика (ИНН);
- копии документов, удостоверяющие личность (паспорт или иной документ);
- копии документов, подтверждающих право на дополнительные гарантии, льготы и компенсации по определенным основаниям (об инвалидности, ветеранстве, нахождении в зоне радиации, службе в подразделениях особого риска, составе семьи, беременности работницы, возрасте детей и т.п.);
- договор гражданско-правового характера между субъектом и лечебным учреждением;
- документы, подтверждающие факты расчетов по договорам;
- личные заявления пациентов.

Соответственно информационные системы МО должны обеспечивать **информационную безопасность** - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера.

Иными словами, любая МИС должна удовлетворять условиям по защите информации, установленным действующим законодательством и обеспечивать возможности разграничения и контроля доступа к системе в целом, отдельным ее функциям и документам на ролевой основе, в том числе для групп пользователей.

**Защита информации** - это комплекс мероприятий, направленных на обеспечение информационной безопасности.

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. 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).

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 записей;
- блокирование доступа к информации;
- несанкционированное 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 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.

**Права доступа пользователей и защита информации**

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 информационной системе 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.**

МИС МО должны поддерживать **следующие функции защиты информации** от несанкционированного доступа:

- аутентификация и авторизация пользователя по логину и паролю условно-постоянного действия;
- управление списками контроля доступа для всех основных объектов МИС МО, включая базы данных, отдельные записи в БД, объекты интерфейса и т.д.;
- изменение прав управления доступом пользователей к ресурсам МИС МО;
- регистрация действий пользователей по доступу к информационным ресурсам и использованию функций МИС МО, любых изменений и запросов к данным, включая их содержание, а также регистрация изменений прав управления доступом;
- регистрация неудачных попыток доступа и изменения системных объектов с сохранением даты и времени, регистрационного имени пользователя системы и типа события в журнале и возможность его анализа;
- обеспечение доступа к данным системы только зарегистрированным авторизованным пользователям, подписавшим специальное соглашение о неразглашении конфиденциальной информации и врачебной тайны.

В рамках внедрения МИС МО должны быть реализованы инфраструктурные сервисы безопасности, обеспечивающие базовый уровень информационной безопасности.

Инфраструктурные сервисы должны обеспечивать:

- идентификацию и авторизацию пользователей;
- управление событиями информационной безопасности;
- инвентаризацию и мониторинг состояния информационной безопасности;
- контроль действий администраторов систем;
- систему антивирусной защиты;
- систему сетевой безопасности, включающую в себя средства межсетевого экранирования, сегментирование сетевой инфраструктуры и инфраструктуры систем хранения, защищенное подключение (VPN).

МИС МО должна обеспечивать защиту персональных данных пациентов на основе ролевого управления доступом, ограничивающего и контролирующего доступ пользователей к информации, содержащей сведения о пациентах.

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:

1)пароль на вход в МИС;

2)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);

3)пароли на модули системы (например, на просмотр и (или) редактирование). 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 пользователей.

Каждый пользователь должен проходить процедуру **аутентификации** (проверка подлинности путём сравнения введённого пароля с паролем, сохранённым в базе данных пользовательских логинов), а затем, при попытках получения доступа к данным, - **авторизацию,** т.е. проверку разрешений пользователя по отношению к какому-либо защищаемому ресурсу. МИС МО должна быть устроена таким образом, чтобы функции, осуществляющие контроль за безопасностью данных, выполнялись прежде, чем разрешается выполнение любой другой функции. МИС МО должна эффективно предотвращать любые попытки доступа к данным со стороны неавторизованных лиц.

В настоящее время одним из эффективных механизмов обеспечения информационной безопасности в МО является использование **электронной подписи** (рис. 14). Электронная подпись (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) и используется для определения лица, подписывающего информацию (Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"). Это позволяет установить автора электронного документа и гарантировать неизменность его содержания.


Рис. Разновидности носителей ЭП, используемые в России.

Выделяют два вида ЭП - простая и усиленная электронная подпись. В свою очередь усиленная ЭП бывает неквалифицированной и квалифицированной. *Простой электронной подписью* является ЭП, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

*Неквалифицированной электронной подписью* является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

*Квалифицированной электронной подписью* является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и, кроме того, следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи.

Информация в электронной форме, подписанная усиленной квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

В настоящее время в российском здравоохранении активно внедряется использование ЭП и одновременно совершенствуется нормативно-правовая база в отношении юридически значимого электронного документооборота.

**Мониторинг состояния информационной безопасности**

В системе должен быть реализован механизм учета автора (и времени) создавшего запись, множественность хранения записей с привязкой ко времени их создания и ко времени корректировки изменений.

МИС МО должна обеспечивать набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных событий, которые могут произойти в системе. Мониторинг относящихся к безопасности событий должен позволять обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к системе или защищаемой информации.

**Сохранность информации при авариях**

Отказы и сбои в работе технических средств рабочих мест пользователей МИС МО, серверов приложений, серверов баз данных и сетевого оборудования не должны приводить к разрушению данных и сказываться на работоспособности МИС МО в целом.

При возникновении сбоев в аппаратном обеспечении, включая аварийное отключение электропитания, МИС МО должна иметь возможность автоматически восстанавливать свою работоспособность после устранения сбоев и корректного перезапуска аппаратного обеспечения (за исключением случаев повреждения рабочих носителей информации с исполняемым программным кодом).

МИС МО должна обеспечивать корректную обработку ошибочных ситуаций с дальнейшим продолжением работы без аварийного закрытия подсистем, за исключением случаев, когда ошибка делает дальнейшую работу в рамках пользовательской сессии невозможной. В случае сбоя операционной системы или сервера в процессе выполнения пользовательских задач должно быть обеспечено восстановление данных в базе данных до состояния на момент окончания последней нормально завершенной операции. Должна быть предусмотрена возможность автоматического или ручного резервного копирования данных баз данных МИС МО (в том числе и на удаленное хранилище).

## ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1) Что такое конфиденциальная информация?
2) Дайте определение информационной безопасности.
3) Что такое защита информации?
4) Дайте определение информационной угрозе.
5) Какие медицинские данные требуют защиты?
6) Что такое авторизация и аутентификация пользователей?
7) Как организуется система паролей для обеспечения конфиденциальности данных?
8) Что такое электронная подпись?
9) Какие виды ЭП существуют?
10) Как осуществляется мониторинг состояния информационной безопасности.
11) Каким образом обеспечивается сохранность информации при отказах и сбоях?