ПРОТОКОЛ № 3

заседания Общественного совета
при ГУЗ «Тульская областная клиническая больница № 2 им. Л.Н. Толстого»
г. Тула 25 сентября 2025 г.

Место проведения: ГУЗ «Тульская областная больница № 2 им. Л.Н. Толстого», г. Тула, ул. Тимирязева, д.27, конференц-зал.

Время проведения: 12 час.00 мин.

Председательствовал: Богданова Т.В.

Присутствовали: Лаврова О.В., Волкова Т.Н., Шишкова А.Н., Дубинин А.Э., Озеров В.В., представители общественности, представители трудового коллектива.
Секретарь совета: Кучернюк Ю.А.

Повестка дня:

1. Защита персональных данных в учреждении.
По первому вопросу выступил Аннушкин И.А., начальник информационного отдела¸

Закон о персональных данных вступил в силу с 2006 года и многие организации уже сталкивались с контролирующими органами по вопросам выполнения требований законодательства. Персональные данные - это информация которая относится к тому или иному субъекту персональных данных, физическому лицу. Это может быть имя, адрес электронной почты, номер телефона, адрес проживания, паспортные данные данные, СНИЛС, полис страхования и так далее.
Основным контролирующим органом в сфере обработки персональных данных является Роскомнадзор, он контролирует деятельность операторов персональных данных. Помимо этого, другими контролирующими органами являются Федеральная служба по техническому и экспортному контролю (ФСТЭК) и Федеральная Служба Безопасности (ФСБ). Роскомнадзор в целом контролирует полное соблюдение законодательства о персональных данных, трансграничную передачу данных, ФСБ отвечает за эксплуатацию средств криптографической защиты информации, а ФСТЭК - за техническую защиту информации.
Как больнице выполнить требования по защите персональных данных пациентов
Чтобы больнице соответствовать требованиям ФЗ-152, необходимо следовать четкому порядку действий: Провести аудит информационной системы. Нужно понять, где обрабатываются персональные данные, на каких компьютерах, на каких серверах, в каком виде. После этого определить угрозы безопасности персональных данных. Если у вас большая информационная система, нужно разработать технические параметры системы защиты информации (приказы, инструкции, журналы). Всё это требуется в соответствии с Законодательством, а грамотное ведение документации проверяет Роскомнадзор. Следующим шагом необходимо определить технические мероприятия по защите информации и провести аттестацию информационной системы по требованиям безопасности информации. При этом чтобы выполнить весь блок мероприятий, необходимо очень четко понимать, какие нормативно-правовые акты к вам в целом применимы, какие требования законодательства вы должны выполнять. Медицинская организация обязана выполнять целый ряд требований законодательства ФЗ-152, приказ ФСТЭК № 21, приказ ФСБ №378, который определяет меры по криптографической защите информации. Но помимо этого есть множество документов от Минздрава, которые медицинские организации должны соблюдать, в частности методические рекомендации по организации взаимодействия медорганизаций с ЕГИСЗ.
Какие требования по защите информации должна выполнять клиника с точки зрения законодательства?
Во-первых надо выполнять требования по защите информационных систем это приказ ФСТЭК №17 и приказ правительства 911н. Сама медицинская информационная система

должна иметь подтверждение соответствия требованиям безопасности. Это может быть либо оценка эффективности, либо аттестация информационной системы. Кроме того, средства защиты информации, в том числе средства криптографической защиты информации должны обязательно быть сертифицированы.
Основные меры по защите информации, которые необходимо обеспечить больнице: требования по идентификации и аутентификации¸ защита машинных носителей информации, антивирусная защита, анализ защищенности персональных данных, защита среды виртуализации¸защита технических средств.
Исходя из этого появляется блок средств защиты информации, которые должны быть внедрены в больнице: средства защиты от несанкционированного доступа , средства антивирусной защиты , средства защиты среды визуализации, межсетевые экраны, средства криптографической защиты информации.

Аннушкин И.А. проинформировал о плане мероприятий учреждения по объектам критической инфраструктуры, который осуществляется в целях защиты персональных данных.
План мероприятий по объектам критической инфраструктуры (КИИ) – это документ, определяющий действия, необходимые для обеспечения безопасности КИИ и предотвращения возможных угроз утечки персональных данных, например, кибератак или техногенных катастроф. Он включает в себя перечень задач, ответственных исполнителей, сроки выполнения и ожидаемые результаты.

Основные этапы разработки и реализации плана мероприятий по КИИ:

1. **1. Анализ и категорирование объектов КИИ:**

- Выявление и оценка значимости объектов КИИ, которые могут быть подвергнуты угрозам.
- Определение уровня значимости (например, по шкале от 1 до 5) на основании анализа потенциального ущерба от их нарушения.
- Выявление критических точек и уязвимостей на каждом объекте КИИ.

2. Разработка плана мероприятий:

- Для каждого объекта КИИ определяется перечень мер, направленных на обеспечение безопасности, например, внедрение системы безопасности, контроль доступа, мониторинг инцидентов, обучение персонала и т.д.
- Указываются ответственные за выполнение каждой меры, сроки и ожидаемые результаты.
- План должен включать меры по предотвращению, выявлению, реагированию и ликвидации последствий.

3. Внедрение и контроль:

- Реализация запланированных мер, например, установка оборудования, внедрение политик безопасности, проведение тренировок.
- Регулярный контроль за выполнением плана, мониторинг эффективности мер безопасности и корректировка плана при необходимости.
- Проведение проверок и аудитов для оценки соответствия плана требованиям безопасности.

Примеры мероприятий по обеспечению безопасности КИИ:

- **Технические меры:**

  внедрение систем безопасности, контроль доступа, мониторинг и обнаружение инцидентов, защита от кибератак.

- **Организационные меры:**

  разработка и внедрение политик безопасности, обучение персонала, создание служб безопасности, планирование реагирования на инциденты.

- **Процедурные меры:**

  разработка и внедрение процедур по управлению рисками, реагированию на инциденты, и аварийному восстановлению.
  Ответственность за реализацию плана мероприятий.

2. Подготовка учреждения к зиме.

По второму вопросу выступил Дубинин А.Э., заместитель главного врача по хозяйственным вопросам, который рассказал о подготовке учреждения к работе в зимнее время.

В учреждении были проведены следующие работы:
Отделение в Ясной Поляне:
-ремонт и опрессовка системы отопления
-утепление чердаков дневного стационара и терапевтического корпуса
-утепление подвала в прачечной
-ремонт входной двери в поликлинике и в здании дневного стационара
-ремонт порогов поликлиники
-регулировка окон в хирургическом отделении и лаборатории.

Филиал № 1:
- ремонт и опрессовка системы отопления;
- проведение мелкого ремонта радиаторов отопления;
- текущий ремонт и укрепление стен стационара;
- замена по гарантии радиаторов отопления в поликлинике.
Проблемный момент: состояние кровли и стен в стационаре, нуждающихся в капитальном ремонте.

Выводы: Признать работу Общественного совета ГУЗ «ТОКБ № 2 им. Л.Н. Толстого» за 9 мес. 2025 г. удовлетворительной. Продолжать реализацию мер общественного контроля в учреждении.

Председатель Общественного совета: Богданова Т.В.
Секретарь заседания: Кучернюк Ю.А.