

**Заявка**  
**на изготовление информационного стенда**  
**(размер - 1м x 2м)**

Требования к тексту и фото:

- *Общий объем текста в формате .doc - **не более 1000 знаков.***
- *Фотографии в любом растровом формате (.jpg, .tif, .psd, .bmp), в наибольшем разрешении и размере (не менее 0,5 Мб). **Фотографии необходимо пересылать отдельно в исходном формате (в .doc не вставлять)!***

Название разработки	СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ НА ОСНОВЕ PDCA-МОДЕЛИ
Институт СФУ	Институт космических и информационных технологий
Область применения	Информационные системы медицинских учреждений
Авторский коллектив	М.М. Кучеров, канд. физ.-мат. наук (руководитель) Е.А. Кресан
Краткое описание разработки	В рамках данной работы предлагается комплексная методика построения защищенной информационной системы медицинского учреждения в свете международных и российских стандартов в сфере информационных технологий, а так же обеспечение безопасности персональных данных.
Актуальность решаемой задачи (проблемы)	Сведения о состоянии здоровья человека являются конфиденциальной информацией, а их защищенность в медицинских учреждениях гарантируется. Настоящее законодательство, в сфере медицины, достаточно четко регулирует вопросы безопасности информации в целом и защиты персональных данных в частности. Федеральный закон №152-ФЗ относит сведения о состоянии здоровья к специальной категории персональных данных, которые находятся под особой защитой. В основу описания жизненного цикла системы управления информационной безопасностью (СУИБ) положена полициклическая PDCA-модель. Все процедуры системы управления последовательно проходят четыре этапа: планирование, внедрение, мониторинг и анализ, совершенствование. Каждый этап характеризуется выполнением ряда различных процедур.
Конкретные результаты (эффекты)	Основные вехи построения СУИБ на сегодняшний день: <ul style="list-style-type: none"> <li>• Внутренний аудит ИБ, и определения вектора развития ИС.</li> <li>• Создание концепции ИБ.</li> <li>• Разработка и ввод в эксплуатацию системы резервного копирования.</li> <li>• Разработка программы обучения пользователей ИС основам ИБ.</li> </ul> Срок реализации: менее 1 года. В результате применения методики удастся значительно повысить уровень защищенности как информационной системы в целом, так и подсистемы обработки персональных данных в частности.
Перспективы продолжения работы (если есть)	Перспективность продолжения работы заложена на стадии проектирования – процесс совершенствования системы непрерывен.

Заполненные заявки фото(отдельно!) необходимо отправить по электронной почте:  
[expo@sfu-kras.ru](mailto:expo@sfu-kras.ru).

Контакт. телефон 2912886 (Сергоманова Галина Михайловна).

### Образец стенда

область применения	ИНФОРМАЦИОННЫЕ СИСТЕМЫ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ
	
авторский коллектив	СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ НА ОСНОВЕ PDCA-МОДЕЛИ  М.М. Кучеров, канд. физ.-мат. наук (руководитель) Е.А. Кресан
	<b>Актуальность</b> Сведения о состоянии здоровья человека являются конфиденциальной информацией, а их защищенность в медицинских учреждениях гарантируется. Предлагается комплексная методика построения защищенной информационной системы медицинского учреждения в свете международных и российских стандартов в сфере информационных технологий, а так же обеспечение безопасности персональных данных.
	В основу описания жизненного цикла системы управления информационной безопасностью (СУИБ) положена полициклическая PDCA-модель. Все процедуры системы управления последовательно проходят четыре этапа: планирование, внедрение, мониторинг и анализ, совершенствование. Каждый этап характеризуется выполнением ряда различных процедур. <b>Основные вехи построения СУИБ на сегодняшний день:</b> <ul style="list-style-type: none"><li>• Внутренний аудит ИБ, и определения вектора развития ИС.</li><li>• Создание концепции ИБ.</li><li>• Разработка и ввод в эксплуатацию системы резервного копирования.</li><li>• Разработка программы обучения пользователей ИС основам ИБ.</li></ul>
→	<b>Срок реализации</b> менее 1 года. В результате применения методики удается значительно повысить уровень защищенности как информационной системы в целом, так и подсистемы обработки персональных данных в частности.
СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ SIBERIAN FEDERAL UNIVERSITY  Институт космических и информационных технологий	