

АННОТАЦИЯ
образовательной программы
по специальности:

10.05.02 "Информационная безопасность телекоммуникационных систем"

Язык, на котором осуществляется обучение: русский	
Форма и срок обучения	Очная форма - 5,5 лет
Будущая квалификация	Специалист по направлению подготовки «Информационная безопасность телекоммуникационных систем»
Специализация	<i>Разработка защищённых телекоммуникационных систем</i>
Будущие профессии	Инженер по защите информации Специалист организационно-правовой защиты информации Специалист по обслуживанию сетей телекоммуникаций Специалист по технической защите информации Специалист программно-аппаратной защиты информации Проектировщик защищённых телекоммуникационных сетей Разработчик оборудования и программно-аппаратных модулей защиты информации Специалист по радиомониторингу
Чему научат?	<ul style="list-style-type: none">• Выявлять возможные источники и технические каналы утечки информации, представляющие государственную, военную, служебную или коммерческую тайну• Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности• Прогнозировать и моделировать информационные угрозы телекоммуникационных систем, оценивать уровни риска• Программировать на различных языках С, С++, С# и других.• Изучать и обобщать опыт работы учреждений по использованию технических средств и способов защиты информации в телекоммуникационных системах• Участвовать в разработке компонентов телекоммуникационных систем (систем связи для передачи и обработки информации: телефонных сетей, радио- и мобильной связи, компьютерных сетей, кабельного телевидения и других)• Проектировать защищённые информационно-телекоммуникационные системы• Рационально выбирать элементную базу при проектировании устройств и систем защиты информации телекоммуникационных систем• Строить эффективные модели сигналов, помех и каналов связи, знать способы формирования и

преобразования сигналов в телекоммуникационных системах

- Проверять работоспособность и эффективность применяемых программно-аппаратных (средства авторизации, антивирусные средства, системы обнаружения и предотвращения вторжений, системы аутентификации), криптографических (шифрование, цифровая подпись) и технических средств (звукоизоляция помещений, приборы по зашумлению или по выявлению устройств перехвата информации) защиты информации
- Восстанавливать работу систем защиты информации при сбоях и нарушениях
- Оценивать эффективность систем защиты информации в телекоммуникационных системах
- Осуществлять аудит уровня защищенности и аттестацию телекоммуникационных систем
- Разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы
- Оценивать затраты и результаты деятельности организации по обеспечению информационной безопасности
- Составлять правила, положения, инструкции и другие организационно-распорядительные документы для управления информационной безопасностью телекоммуникационных систем
- Применять законы в области обеспечения информационной безопасности
- Читать техническую документацию на иностранных языках

**Базовые
профессиональные
дисциплины**

Информационная безопасность телекоммуникационных систем | Программно-аппаратные средства обеспечения информационной безопасности | Управление информационной безопасностью | Математические основы криптологии | Криптографические методы защиты информации | Техническая защита информации | Сети и системы передачи информации | Проектирование защищённых телекоммуникационных систем | Защита программных средств защищённых телекоммуникационных систем | Организационно-правовое обеспечение информационной безопасности | Электроника и схемотехника | Теория электрических цепей | Теория электрической связи | Информационные технологии | Технология и методы программирования | Языки программирования | Теория информации | Аппаратные средства телекоммуникационных систем | Квантовая и оптическая электроника | Измерения в

телекоммуникационных системах | Теория принятия решений в условиях информационных конфликтов | Цифровая обработка сигналов | Моделирование систем и сетей телекоммуникаций | Радиомониторинг | Квантовая связь и криптография

Практика студентов

Учебную и производственную практики студенты могут проходить в любых организациях (в службах экономической безопасности, режимных отделах, службах информационной безопасности, отделах кадров), где используются технические средства обработки, хранения и передачи конфиденциальной информации, в том числе в органах государственной власти, силовых структурах (МВД, ФСБ, таможенной службе, налоговых органах), медицинских учреждениях, банках, СМИ, предприятиях телекоммуникации и связи.

Итоговая аттестация

Защита дипломного проекта

Военная подготовка

Возможность обучения в военном учебном центре ЮФУ (контракт заключается при поступлении), возможность обучения на факультете военного обучения по программам подготовки офицеров запаса (2-4 курсы).

Общежитие

Иногородним предоставляются места в общежитиях