

МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ПРИКАЗ

«24» июля 2017 г.

№ 229-02

г. Ростов-на-Дону

**Об утверждении образовательного стандарта
Южного федерального университета по направлению подготовки
10.05.02 Информационная безопасность телекоммуникационных систем**

На основании решения Ученого совета ЮФУ от 30 июня 2017 года
(Протокол № 6) п р и к а з ы в а ю:

1. Утвердить прилагаемый образовательный стандарт Южного федерального университета по направлению подготовки 10.05.02 Информационная безопасность телекоммуникационных систем.

2. Структурным подразделениям, реализующим образовательные программы по направлению подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, привести образовательные программы в соответствие с требованиями прилагаемого образовательного стандарта ЮФУ в срок до 1 сентября 2017 года.

3. Обучающихся всех курсов и форм обучения по направлению подготовки 10.05.02 Информационная безопасность телекоммуникационных систем перевести с 1 сентября 2017 года на образовательные программы, соответствующие требованиям прилагаемого образовательного стандарта ЮФУ.

4. Контроль исполнения настоящего приказа возложить на проректора по методической работе – ответственного секретаря приемной комиссии Г.Р. Ломакину.

Ректор



М.А. Боровская

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное автономное образовательное учреждение высшего образования
«Южный федеральный университет»

Утвержден приказом Южного
федерального университета
от «30» мая 2017 г. № 229-ОД

Принят Ученым советом ЮФУ

«30» мая 2017 г.

Протокол № 6

Главный ученый секретарь М.С. О.С. Мирошниченко

**ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ
ВЫСШЕГО ОБРАЗОВАНИЯ
ЮЖНОГО ФЕДЕРАЛЬНОГО УНИВЕРСИТЕТА**

Уровень высшего образования

специалитет

Специальность

10.05.02 Информационная безопасность телекоммуникационных систем

г. Ростов-на-Дону,
2017

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Образовательный стандарт высшего образования Южного федерального университета (далее ЮФУ) представляет собой совокупность требований, обязательных при реализации основных профессиональных образовательных программ подготовки специалистов по специальности **10.05.02 Информационная безопасность телекоммуникационных систем** в ЮФУ в соответствии с лицензией на право ведения образовательной деятельности.

1.2. Порядок разработки, утверждения и внесения изменений в образовательный стандарт ЮФУ определяется Положением об образовательных стандартах Южного федерального университета, разработанных и утверждённых самостоятельно (приказ от «18» мая 2016 г. № 196-ОД).

1.3. Нормативная правовая база разработки образовательного стандарта ЮФУ:
Федеральный закон: «Об образовании в Российской Федерации» от 29 декабря 2012 года № 273-ФЗ;

Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по специальности 10.05.02 Информационная безопасность телекоммуникационных систем (квалификация (степень) «специалист»), утверждённый приказом Министерства образования и науки Российской Федерации от «16» ноября 2016 г. № 1426;

Профессиональные стандарты (Приложение № 1);

Всемирная инициатива CDIO. Стандарты;

Всемирная инициатива CDIO. Планируемые результаты обучения (CDIO Syllabus);

Устав Южного федерального университета;

Стандарт проектирования и реализации образовательных программ Южного федерального университета, утверждённый приказом Южного федерального университета от 27 января 2016 г. № 15-ОД;

Локальные акты Южного федерального университета.

II. ХАРАКТЕРИСТИКА СПЕЦИАЛЬНОСТИ

2.1. Получение образования по программе специалитета допускается только в образовательной организации высшего образования.

2.2. Обучение по программе специалитета в ЮФУ осуществляется только в очной форме обучения.

Объем программы специалитета составляет 330 зачетных единиц (далее – з.е.) вне зависимости от формы обучения, применяемых образовательных технологий, реализации программы специалитета с использованием сетевой формы, реализации программы специалитета по индивидуальному учебному плану, в том числе ускоренному обучению.

2.3. Срок получения образования по программе специалитета:

в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, вне зависимости от применяемых образовательных технологий, составляет 5,5 лет. Объем программы специалитета в очной форме обучения, реализуемый за один учебный год, составляет 60 з.е.;

при обучении по индивидуальному учебному вне зависимости от формы обучения плану устанавливается ЮФУ, но не более срока получения образования, установленного для очной формы обучения. При обучении по индивидуальному плану лиц с ограниченными возможностями здоровья срок может быть увеличен по их желанию, но не более чем на один год по сравнению со сроком, установленным для очной формы обучения. Объем программы специалитета за один учебный год при обучении по индивидуальному плану при очной форме обучения не может составлять более 75 з.е.

2.4. При реализации программы специалитета могут применяться электронное обучение и дистанционные образовательные технологии. При обучении лиц с ограниченными возможностями здоровья электронное обучение и дистанционные образовательные технологии должны предусматривать возможность приёма-передачи информации в доступных для них формах.

По данной специальности не допускается реализация программ специалитета

с применением исключительно электронного обучения, дистанционных образовательных технологий.

2.5. Реализация программы специалитета возможна с использованием сетевой формы.

2.6. Образовательная деятельность по программе специалитета осуществляется на государственном языке Российской Федерации, если иное не определено локальным нормативным актом ЮФУ.

III. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ СПЕЦИАЛИСТОВ

3.1. Область профессиональной деятельности выпускников, освоивших программу специалитета, включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с проектированием, созданием, исследованием и эксплуатацией систем обеспечения информационной безопасности телекоммуникационных систем в условиях существования угроз в информационной сфере.

3.2. Объектами профессиональной деятельности выпускников, освоивших программу специалитета, являются: методы, средства и системы обеспечения информационной безопасности информационно-телекоммуникационных сетей и систем; управление информационной безопасностью информационно-телекоммуникационных сетей и систем; информационно-телекоммуникационные сети и системы различного назначения, их оборудование, принципы построения.

3.3. Виды профессиональной деятельности, к которым готовится выпускник, освоивший программу специалитета:

научно-исследовательская;

проектная;

контрольно-аналитическая;

организационно-управленческая;

эксплуатационная;

инженерно-предпринимательская.

При разработке и реализации программы специалитета разработчики образовательной программы ориентируются на конкретные виды профессиональной деятельности, к которым готовится выпускник, исходя из потребностей рынка труда, научно-исследовательских и материально-технических ресурсов ЮФУ.

Специализации, по которым готовятся выпускники, освоившие программу специалитета:

специализация № 1 «Разработка защищённых телекоммуникационных систем»;

специализация № 2 «Системы подвижной цифровой защищённой связи»;

специализация № 3 «Защита информации в радиосвязи и телерадиовещании»;

специализация № 4 «Защита информации в системах связи и управления»;

специализация № 5 «Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте»;

специализация № 6 «Безопасность телекоммуникационных систем информационного взаимодействия».

3.4. Выпускник, освоивший программу специалитета, в соответствии с видами профессиональной деятельности, на которые ориентирована программа специалитета, должен быть готов решать следующие профессиональные задачи:

научно-исследовательская деятельность:

сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности телекоммуникационных систем, выработка предложений по вопросам комплексного обеспечения информационной безопасности таких систем;

подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;

изучение, анализ и обобщение опыта работы учреждений, организаций и предприятий по использованию технических средств и способов защиты информации в телекоммуникационных системах с целью обеспечения требуемого качества обслуживания, повышения эффективности и совершенствования работ по её защите;

сопровождение разработки, исследование телекоммуникационных систем, сетей и устройств, технических и программно-аппаратных средств защиты и обработки информации в телекоммуникационных системах;

определение требований по защите информации, анализ защищённости телекоммуникационных систем и оценка рисков нарушения их информационной безопасности;

проектная деятельность:

сбор и анализ исходных данных для проектирования систем и средств защиты информации, обеспечения требуемого качества обслуживания в телекоммуникационных системах;

сравнительный анализ сетей и систем передачи информации по показателям информационной безопасности, обеспечения требуемого качества обслуживания;

разработка проектов, технических заданий, планов и графиков проведения работ по защите информации телекоммуникационных систем и необходимой технической документации;

рациональный выбор элементной базы при проектировании систем и средств защиты информации, обеспечения требуемого качества обслуживания телекоммуникационных систем;

разработка политики безопасности, выбор методов и средств обеспечения информационной безопасности объектов информационно-телекоммуникационных систем;

контрольно-аналитическая деятельность:

проверка работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты информации телекоммуникационных средств и систем;

составление методик расчетов и программ экспериментальных исследований по защите информации телекоммуникационных систем, выполнение расчётов в соответствии с разработанными методиками и программами;

проверка учреждений, организаций и предприятий на соответствие требованиям нормативной правовой базы в области информационной безопасности

телекоммуникационных систем;

подготовка отзывов и заключений на нормативно-методические материалы и техническую документацию;

участие в проведении аттестации телекоммуникационных систем, технических средств защиты информации по требованиям соответствующих классов (уровней) безопасности;

организационно-управленческая деятельность:

организация работы коллектива исполнителей, принятие управленческих решений, определение порядка выполнения работ;

разработка предложений по совершенствованию и повышению эффективности комплекса мер по обеспечению информационной безопасности телекоммуникационной системы;

организация работ по выполнению требований режима защиты информации ограниченного доступа;

разработка методических материалов и организационно-распорядительных документов по обеспечению информационной безопасности телекоммуникационных систем на предприятиях;

эксплуатационная деятельность:

эксплуатация технических и программно-аппаратных средств защищённых телекоммуникационных сетей и систем;

документационное обеспечение эксплуатации защищённых телекоммуникационных сетей и систем;

инструментальный мониторинг защищённости телекоммуникационных систем, обеспечения требуемого качества обслуживания;

выявление возможных источников и технических каналов утечки информации;

обеспечение восстановления работоспособности телекоммуникационных систем, в том числе подсистемы защиты информации, при сбоях и нарушении функционирования;

инженерно-предпринимательская деятельность:

осуществление планирования, проектирования, производства и применения продукции профессиональной деятельности в рамках решения задач предприятия, общества и окружающей среды;

создание предприятия, организация и управление его работой, разработка бизнес-планов предприятия, управление капитализацией компании и её финансами;

маркетинг инновационной продукции, планирование производства продукции и услуг с использованием инновационных технологий;

формирование команды предприятия и стимулирование инженерных процессов;

управление интеллектуальной собственностью;

в соответствии со специализациями:

специализация № 1 «Разработка защищённых телекоммуникационных систем»:

разработка алгоритмов преобразования информации и сигналов для защищённых телекоммуникационных систем на основе теоретико-числовых методов;

разработка аппаратного и программного обеспечения узлов и устройств защищённых телекоммуникационных систем на базе сигнальных процессоров;

участие в разработке систем управления информационной безопасностью телекоммуникационных систем, в том числе выбор методов и разработка алгоритмов принятия решений;

специализация № 2 «Системы подвижной цифровой защищённой связи»:

выбор методов, разработка и реализация алгоритмов обработки информации и сигналов для обеспечения безопасности систем подвижной цифровой защищённой связи (далее – СПЦЗС);

разработка узлов и устройств, минимизирующих информационные риски и увеличивающие живучесть СПЦЗС, в том числе модификация аппаратного и программного обеспечения;

контроль работоспособности и определение эффективности средств защиты информации в СПЦЗС;

специализация № 3 «Защита информации в радиосвязи и телерадиовещании»:

участие в процедурах назначения, распределения и эффективного использования радиочастотного спектра;

проведение измерений основных характеристик и параметров телекоммуникационных систем с целью оценки их соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов;

разработка систем, сетей и устройств защищённой радиосвязи и телерадиовещания;

специализация № 4 «Защита информации в системах связи и управления»:

оценка уровня защищённости, в том числе возможностей средств технических разведок применительно к системам связи, управления и объектам информатизации;

обеспечение эффективного применения средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи;

применение методов и средств для закрытия возможных каналов перехвата акустической речевой информации;

специализация № 5 «Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте»:

проведение теоретических и экспериментальных исследований телекоммуникационных систем и сетей транспорта (по видам) и оценка их эффективности;

разработка предложений по совершенствованию системы аудита и управления информационной безопасностью телекоммуникационных систем и сетей транспорта (по видам);

обеспечение эффективной защиты телекоммуникационных систем и сетей транспорта (по видам);

специализация № 6 «Безопасность телекоммуникационных систем информационного взаимодействия»:

выбор и построение адекватных математических и алгоритмических моделей для эффективного проектирования телекоммуникационных систем

информационного взаимодействия и систем управления их поведением;

анализ информационных потоков в целях оценки и повышения уровня безопасности информационного взаимодействия;

применение стандартных средств для анализа программного кода с целью оценки уровня его защиты от исследования и поиска несанкционированного или вредоносного вмешательства в работу телекоммуникационных систем информационного взаимодействия.

IV. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4.1. В результате освоения программы специалитета у выпускника должны быть сформированы универсальные, общепрофессиональные, профессиональные и профессионально-специализированные компетенции. Соответствие компетенций, установленных федеральным государственным образовательным стандартом и образовательным стандартом ЮФУ по специальности 10.05.02 Информационная безопасность телекоммуникационных систем представлено в Приложении №2.

4.2. Выпускник, освоивший программу специалитета, должен обладать следующими универсальными компетенциями (УК):

способностью использовать социально-гуманитарные знания, культуру мышления, системный подход и критический анализ при формировании мировоззренческой и гражданской позиции (УК-1);

способностью аргументированно, логически верно и содержательно строить устную и письменную речь, демонстрируя личную и профессиональную культуру, владеть русским и иностранным языками для решения коммуникативных задач во всех сферах общения (УК-2);

способностью работать в команде, принимать организационно-управленческие решения и готовностью нести за них ответственность (УК-3);

способностью к саморазвитию и самосовершенствованию, проявлению творческого подхода, готовностью к повышению своей квалификации и мастерства (УК-4);

способностью использовать экономические и правовые знания в профессиональной и социальной деятельности (УК-5);

способностью соблюдать принципы и нормы толерантного отношения к носителям разных этнокультурных традиций, религиозных и политических взглядов в многонациональном и поликонфессиональном обществе (УК-6);

способностью поддерживать уровень физической подготовки для обеспечения полноценной социальной и профессиональной деятельности, создавать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций (УК-7).

4.3. Выпускник, освоивший программу специалитета, должен обладать следующими общепрофессиональными компетенциями (ОПК):

способностью применять междисциплинарные знания для решения профессиональных задач с учётом смежных областей науки и практики (ОПК-1);

способностью осуществлять проектную деятельность в профессиональной сфере (ОПК-2);

способностью решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности (ОПК-3);

способностью понимать естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять общенаучные методы при решении инженерных задач (ОПК-4);

способностью эффективно применять технические и программные средства и технологии в профессиональной деятельности (ОПК-5);

способностью разрабатывать проектную и отчётную документацию, представлять результаты профессиональной деятельности (ОПК-6);

владеть навыками установки, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ОПК-7);

способностью управлять информационной безопасностью объекта защиты

(ОПК-8);

способностью применять положения теорий радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач (ОПК-9).

4.4. Выпускник, освоивший программу специалитета, должен обладать профессиональными компетенциями (ПК), соответствующими видам профессиональной деятельности:

научно-исследовательская деятельность:

способностью формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов (ПК-1);

способностью оценивать технические возможности и выработать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств (ПК-2);

способностью разрабатывать компоненты телекоммуникационных систем (ПК-3);

проектная деятельность:

способностью проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учётом действующих нормативных и методических документов (ПК-4);

способностью применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-5);

способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учётом предъявляемых к ним требований качества обслуживания и качества функционирования (ПК-6);

контрольно-аналитическая деятельность:

способностью проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем (ПК-7);

способностью проводить аттестацию телекоммуникационных систем по требованиям защиты информации (ПК-8);

способностью оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищённых телекоммуникационных систем, выполнять подготовку соответствующих заключений (ПК-9);

организационно-управленческая деятельность:

способностью организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы (ПК-10);

способностью выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности (ПК-11);

способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем (ПК-12);

эксплуатационная деятельность:

способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-13);

способностью проводить инструментальный мониторинг защищённости телекоммуникационных систем, обеспечения требуемого качества обслуживания (ПК-14).

инженерно-предпринимательская деятельность:

способностью понимать и нести ответственность за принимаемые решения и проектируемые объекты профессиональной деятельности в социально-экономическом контексте инженерной деятельности (ПК-15);

способностью разрабатывать бизнес-планы предприятий профессиональной сферы, осуществлять мероприятия по созданию предприятий, по организации и управлению их работой (ПК-16);

способностью управлять капитализацией компании и её финансами, осуществлять маркетинг инновационной продукции на рынке продуктов и услуг в области информационной безопасности телекоммуникационных систем (ПК-17);

способностью осуществлять планирование производства продукции и (или) услуг с использованием инновационных технологий (ПК-18);

способностью формировать команды и разрабатывать системы стимулирования инженерных процессов (ПК-19);

способностью осуществлять управление интеллектуальной собственностью (ПК-20).

4.5. Выпускник, освоивший программу специалитета, должен обладать **профессионально-специализированными компетенциями** (ПСК), соответствующими специализации программы специалитета:

специализация № 1 «Разработка защищённых телекоммуникационных систем»:

способностью разрабатывать алгоритмы преобразования информации и сигналов для защищённых телекоммуникационных систем на основе теоретико-числовых методов (ПСК-1.1);

способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищённых телекоммуникационных системах (ПСК-1.2);

способностью разрабатывать аппаратное и программное обеспечение узлов и устройств защищённых телекоммуникационных систем на базе сигнальных процессоров (ПСК-1.3);

способностью разрабатывать системы управления информационной безопасностью телекоммуникационных систем (ПСК-1.4);

способностью обеспечивать защиту программных средств защищённых телекоммуникационных систем (ПСК-1.5);

специализация № 2 «Системы подвижной цифровой защищённой связи»:

способностью выбирать методы и разрабатывать алгоритмы для обеспечения безопасности СПЦЗС (ПСК-2.1);

способностью использовать и реализовать современные алгоритмы обработки информации и сигналов в целях обеспечения безопасности СПЦЗС (ПСК-2.2);

способностью модифицировать аппаратное и программное обеспечение узлов и устройств СПЦЗС (ПСК-2.3);

способностью контролировать работоспособность и определять эффективность средств защиты информации в СПЦЗС (ПСК-2.4);

способностью разрабатывать узлы и устройства, минимизирующие информационные риски и увеличивающие живучесть СПЦЗС (ПСК-2.5);

специализация № 3 «Защита информации в радиосвязи и телерадиовещании»:

способностью использовать нормативные правовые акты и нормативные методические документы в области технологий и систем радиосвязи и телерадиовещания (ПСК-3.1);

владеть процедурами назначения, распределения и эффективного использования радиочастотного спектра (ПСК-3.2);

способностью применять методы повышения помехоустойчивости и защищённости систем радиосвязи и телерадиовещания и определять эффективность их использования (ПСК-3.3);

способностью проводить измерения основных характеристик и параметров телекоммуникационных систем с целью оценки их соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов (ПСК-3.4);

способностью разрабатывать системы, сети и устройства защищённой радиосвязи и телерадиовещания (ПСК-3.5);

специализация № 4 «Защита информации в системах связи и управления»:

способностью применять теорию сигналов и систем для анализа

телекоммуникационных систем и оценки их помехоустойчивости (ПСК-4.1);

способностью формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем (ПСК-4.2);

способностью оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации (ПСК-4.3);

способностью применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации (ПСК-4.4);

способностью проводить оценку уровня защищённости и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи (ПСК-4.5);

специализация № 5 «Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте»:

способностью проводить теоретические и экспериментальные исследования телекоммуникационных систем и сетей транспорта (по видам) и оценивать их эффективность (ПСК-5.1);

способностью осуществлять рациональный выбор методов и средств обеспечения информационной безопасности телекоммуникационных систем и сетей транспорта (по видам) (ПСК-5.2);

способностью разрабатывать предложения по совершенствованию системы аудита и управления информационной безопасностью телекоммуникационных систем и сетей транспорта (по видам) (ПСК-5.3);

способностью к профессиональной эксплуатации современного оборудования, использовать методы и средства измерений для решения метрологических задач и технической диагностики защищенных систем и сетей транспорта (по видам) (ПСК-5.4);

способностью обеспечить эффективную защиту телекоммуникационных систем и сетей транспорта (по видам) (ПСК-5.5);

специализация № 6 «Безопасность телекоммуникационных систем

информационного взаимодействия»:

способностью выполнять декомпозицию сложных информационных систем, формулировать показатели их эффективности с целью построения корректной концептуальной модели систем (ПСК-6.1);

способностью обоснованно выбирать и (или) строить адекватные, математические и алгоритмические модели, в том числе с помощью высокоуровневых средств, для эффективного проектирования телекоммуникационных систем информационного взаимодействия (ПСК-6.2);

способностью обоснованно выбирать и применять адекватные методы кодирования для построения высокоэффективных телекоммуникационных систем информационного взаимодействия и систем управления их поведением (ПСК-6.3);

способностью анализировать информационные потоки на пакетном уровне, оценивать реальный уровень безопасности информационного взаимодействия и предлагать эффективные меры для его повышения (ПСК-6.4);

способностью применять стандартные средства для анализа программного кода с целью оценки уровня его защиты от исследования и поиска несанкционированного или вредоносного вмешательства в работу телекоммуникационных систем информационного взаимодействия (ПСК-6.5).

4.6. При разработке программы специалитета все универсальные, общепрофессиональные, профессиональные компетенции, отнесённые к тем видам профессиональной деятельности, на которые ориентирована программа специалитета, и профессионально-специализированные компетенции, отнесённые к выбранной специализации, включаются в набор требуемых результатов освоения программы специалитета.

4.7. При разработке программы специалитета разработчики образовательной программы вправе дополнить набор компетенций выпускников с учётом направленности программы специалитета на конкретные области знания, и (или) виды деятельности, или специализации программы, и (или) с учётом квалификационных требований по соответствующей военно-учётной специальности при подготовке специалистов по заказу Министерства обороны Российской

Федерации.

V. ТРЕБОВАНИЯ К СТРУКТУРЕ ПРОГРАММЫ СПЕЦИАЛИТЕТА

5.1. Структура программы специалитета включает обязательную часть (базовую) и часть, формируемую участниками образовательных отношений (вариативную). Это обеспечивает возможность реализации программ специалитета, имеющих различную направленность (профиль) образования в рамках одной специализации программы специалитета.

5.2. Программа специалитета состоит из следующих блоков:

Блок 1 «Дисциплины (модули)», который включает дисциплины (модули), относящиеся к базовой части программы (в том числе дисциплины (модули) выбранной специализации) и дисциплины (модули), относящиеся к вариативной части программы.

Блок 2 «Практики, в том числе научно-исследовательская работа (НИР)», который в полном объёме относится к вариативной части программы.

Блок 3 «Государственная итоговая аттестация», который в полном объёме относится к базовой части программы и завершается присвоением квалификации «специалист по защите информации».

Таблица 1

Структура программы специалитета

Структура программы специалитета		Объём программы специалитета в зачётных единицах
Блок 1	Дисциплины (модули)	285-291
	Базовая часть, в том числе дисциплины (модули) специализации	201-231
	Вариативная часть	60-90
Блок 2	Практики, в том числе научно-исследовательская работа (НИР)	33-36
	Вариативная часть	33-36

Структура программы специалитета		Объём программы специалитета в зачётных единицах
Блок 3	Государственная итоговая аттестация	6-9
	Базовая часть	6-9
Объём программы специалитета		330

5.3. Дисциплины (модули), включая дисциплины (модули) специализации, относящиеся к базовой части программы специалитета, являются обязательными для освоения обучающимся вне зависимости от направленности (профиля) программы, которую он осваивает. Набор дисциплин (модулей) и практик, относящихся к базовой части программы специалитета, разработчики образовательной программы определяют самостоятельно в объёме, установленном стандартом ЮФУ.

5.4. Блок 1 включает следующие обязательные модули дисциплин:

Модуль общеуниверситетских дисциплин, который включает дисциплины (модули) являющиеся обязательными для всех направлений подготовки ЮФУ: Иностранный язык; История; Философия; Культура здоровья; Безопасность жизнедеятельности; Экономико-правовое обеспечение инженерной деятельности.

Модуль проектной деятельности, включающий дисциплины и творческие проекты, направленные на решение профессионально-ориентированных задач: Введение в инженерную деятельность, 8 з.е., дисциплина реализуется с 1 по 4 семестры, в рамках дисциплины выполняется 2 творческих проекта; Творческий проект, 3 з.е., реализуемый на 3 курсе; Творческий проект, 3 з.е., реализуемый на 4 курсе.

Модуль университетской академической мобильности (вариативная часть), позволяющий дополнить образовательную программу базовыми знаниями, умениями и навыками из других предметных областей. Модуль включает в себя три набора дисциплин по выбору студента, трудоёмкостью по 5 з.е. каждая, реализуемые на 2 и 3 курсах.

При реализации программы, ориентированной на подготовку специалистов по

заказу Министерства обороны Российской Федерации, вместо Модуля университетской академической мобильности в ОПОП вводится **Модуль военной подготовки (вариативная часть)**, включающий обязательные дисциплины вариативной части, определяемые программой подготовки специалистов по заказу Министерства обороны Российской Федерации, по результатам которого проводится итоговая аттестация по военной подготовке в форме сдачи итогового междисциплинарного экзамена.

При реализации программ, в которых одним из видов деятельности выбрана инженерно-предпринимательская деятельность, вместо Модуля университетской академической мобильности в ОПОП вводится **Модуль инженерного предпринимательства**, содержание которого направлено на формирование компетенций инженерно-предпринимательского вида деятельности.

Модуль общепрофессиональных дисциплин, включающий дисциплины по: математике; физике; дискретной математике; основам алгоритмизации и программирования; математической логике и теории алгоритмов; операционным системам; электротехнике, электронике и схемотехнике; аппаратным средствам и вычислительной технике; стандартам и оформлению инженерной документации, теории информации и другие дисциплины, направленные на освоение общепрофессиональных компетенций;

Модуль профессиональных дисциплин, включающий дисциплины по: мультисервисным сетям; криптографическим методам защиты информации; основам информационной безопасности; организационному и правовому обеспечению информационной безопасности; технической защите информации и другие дисциплины, направленные на освоение профессиональных компетенций.

Модуль по физической культуре и спорту реализуется дисциплинами:

- базовой части Блока 1 (дисциплина Культура здоровья в объёме не менее 72 академических часов (2 зачётные единицы) в очной форме обучения);
- elective дисциплинами в объёме не менее 328 академических часов, которые являются обязательными для освоения и в зачётные единицы не переводятся.

Для инвалидов и лиц с ограниченными возможностями здоровья модуль по физической культуре и спорту должен учитывать состояние здоровья и требования по доступности.

5.5. В Блок 1 могут входить и другие модули образовательной программы, относящиеся к базовой или вариативной частям образовательной программы. Данные модули разрабатываются с учетом направленности (профиля) и специализации программы, выбранных вида (видов) профессиональной деятельности в объеме, установленном настоящим стандартом. После выбора обучающимся направленности (профиля) и специализации программы, набор соответствующих дисциплин (модулей) становится обязательным для освоения обучающимся.

Трудоёмкость всех дисциплин, кроме указанных в модуле общеуниверситетских дисциплин, модуле проектной деятельности и модуле военной подготовки, должна быть не менее 5 з.е.

5.6. В Блок 2 входят учебная, производственная, в том числе преддипломная, практики.

Типы учебной практики:

практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности;

учебно-лабораторный практикум;

ознакомительная практика;

экспериментально-исследовательская практика.

Типы производственной практики:

практика по получению профессиональных умений и опыта профессиональной деятельности по специальности;

научно-исследовательская работа.

Способы проведения учебной и производственной практик:

стационарная; выездная.

Преддипломная практика проводится для выполнения выпускной квалификационной работы и является обязательной.

При разработке программы специалитета разработчики выбирают типы практик в зависимости от вида (видов) деятельности, на который (которые) ориентирована программа специалитета и специализации программы. Разработчики программы вправе предусмотреть иные типы практик дополнительно к установленным настоящим стандартом.

Учебная и (или) производственная практики могут проводиться в структурных подразделениях ЮФУ.

При реализации программы, ориентированной на подготовку специалистов по заказу Министерства обороны Российской Федерации, допускается проведение учебной практики в виде учебных сборов, а части производственной практики в виде войсковой стажировки.

Для лиц с ограниченными возможностями здоровья выбор мест прохождения практик должен учитывать состояние здоровья и требования по доступности.

5.7. В Блок 3 «Государственная итоговая аттестация» входит защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, а также подготовка к сдаче и сдача государственного экзамена, который включается в состав государственной итоговой аттестации по решению учёного совета структурного подразделения.

5.8. Программы специалитета, содержащие сведения, составляющие государственную тайну, разрабатываются и реализуются с соблюдением требований, предусмотренных законодательством Российской Федерации и нормативными правовыми актами в области защиты государственной тайны.

5.9. Реализация части (частей) образовательной программы и государственной итоговой аттестации, в рамках которой (которых) до обучающихся доводятся сведения ограниченного доступа и (или) в учебных целях используются секретные образцы вооружения, военной техники, их комплектующие изделия, не допускается с применением электронного обучения, дистанционных образовательных технологий.

5.10. При разработке программы специалитета обучающимся обеспечивается возможность освоения дисциплин (модулей) по выбору, в том числе специальные

условия инвалидам и лицам с ограниченными возможностями здоровья в объёме не менее 30 процентов вариативной части Блока 1 «Дисциплины (модули)».

5.11. Количество часов, отведенных на занятия лекционного типа, в целом по Блоку 1 «Дисциплины (модули)» должно составлять не более 50 процентов от общего количества часов аудиторных занятий, отведенных на реализацию данного Блока.

5.12. Максимальный объем занятий обучающегося с применением электронного обучения, дистанционных образовательных технологий не должен превышать 25 процентов объема Блока 1 «Дисциплины (модули)».

VI. ТРЕБОВАНИЯ К УСЛОВИЯМ РЕАЛИЗАЦИИ ПРОГРАММЫ СПЕЦИАЛИТЕТА

6.1. Общесистемные требования к реализации программы специалитета.

6.1.1. ЮФУ обеспечивает для обучающихся возможность формирования собственной образовательной программы обучения, включая возможность разработки индивидуальных образовательных программ и (или) траекторий.

6.1.2. ЮФУ создаёт условия для успешной реализации ОПОП специалитета с учётом требований международных стандартов инженерного образования CDIO. Условия реализации ОПОП специалитета должны обеспечивать интеграцию учебного процесса, проектной, научной и практической деятельности посредством социального партнёрства, взаимодействия ЮФУ с корпоративной (отраслевой) наукой, производством, бизнесом, социальной сферой, участия работодателей в разработке и реализации образовательных программ. Формирование у обучающихся компетенций, необходимых для практической реализации инновационного цикла, включающего стадии осмысления и планирования, проектирования и конструирования, производства и эксплуатации, применительно к широкому спектру высокотехнологичных наукоёмких изделий, а также компетенций, требуемых для инжинирингового сопровождения жизненного цикла таких систем должно поддерживаться необходимым материально-техническим, кадровым, организационным и учебно-методическим обеспечением учебного процесса по

реализуемым ОПОП специалитета, а также к применяемым образовательными технологиями.

6.1.3. Для реализации компетентного подхода при реализации ОПОП специалитета должны широко использоваться активные и интерактивные формы проведения занятий (проектную деятельность, компьютерные симуляции, деловые и ролевые игры, разбор конкретных ситуаций, психологические тренинги и др.) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных и надпрофессиональных навыков обучающихся. В рамках ОПОП специалитета должны быть предусмотрены встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

6.1.4. ЮФУ обеспечивает реализацию ОПОП необходимой материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

6.1.5. Каждый обучающийся в течение всего периода обучения должен быть обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам (электронным библиотекам) и электронной информационно-образовательной среде ЮФУ. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда должны обеспечивать возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), как на территории Университета, так и вне его.

Электронная информационно-образовательная среда ЮФУ должна обеспечивать:

доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах;

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения ОПОП;

проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет».

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, её использующих и поддерживающих. Функционирование электронной информационно-образовательной среды должно соответствовать законодательству Российской Федерации.

6.1.6. В случае реализации программы специалитета в сетевой форме требования к реализации программы специалитета должны обеспечиваться совокупностью ресурсов материально-технического и учебно-методического обеспечения, предоставляемого ЮФУ и организациями-партнерами, участвующими в реализации программы специалитета в сетевой форме.

6.1.7. В случае реализации программы специалитета на созданных в установленном порядке в иных организациях кафедрах и (или) иных структурных подразделениях организации требования к реализации программы специалитета должны обеспечиваться совокупностью ресурсов указанных организаций.

6.1.8. Квалификация руководящих и научно-педагогических работников ЮФУ должна соответствовать квалификационным характеристикам, установленным в Едином квалификационном справочнике должностей руководителей, специалистов и служащих и профессиональным стандартам (при наличии).

6.1.9. Доля штатных научно-педагогических работников (в приведенных к целочисленным значениям ставок) должна составлять не менее 65 процентов от общего количества научно-педагогических работников ЮФУ.

6.1.10. В ЮФУ среднегодовой объём финансирования научных исследований на одного научно-педагогического работника (в приведенных к целочисленным

значениям ставок) должен составлять величину не менее чем величина аналогичного показателя мониторинга системы образования, утверждаемого Министерством образования и науки Российской Федерации.

6.1.11. Среднегодовое число публикаций научно-педагогических работников организации за период реализации программы в расчете на 100 научно-педагогических работников (в приведенных к целочисленным значениям ставок) должно составлять не менее 2 в журналах, индексируемых в базах данных Web of Science или Scopus, или не менее 20 в журналах, индексируемых в Российском индексе научного цитирования.

6.1.12. Право на реализацию программ в области информационной безопасности ЮФУ имеет только при наличии лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну.

6.1.13. В структуре ЮФУ должна быть отдельная выпускающая кафедра или иное структурное подразделение, обеспечивающее образовательную деятельность по реализуемой программе по специальности 10.05.02 Информационная безопасность телекоммуникационных систем.

6.2. Требования к кадровым условиям реализации программы специалитета.

6.2.1. Реализация программы специалитета обеспечивается руководящими и научно-педагогическими работниками ЮФУ, а также лицами, привлекаемыми к реализации программы специалитета на условиях гражданско-правового договора.

6.2.2. Доля научно-педагогических работников (в приведённых к целочисленным значениям ставок), имеющих образование, соответствующее профилю преподаваемой дисциплины (модуля), в общем числе научно-педагогических работников, реализующих программу специалитета, должна составлять не менее 80 процентов.

6.2.3. Доля научно-педагогических работников (в приведённых к целочисленным значениям ставок), имеющих учёную степень (в том числе учёную степень, присвоенную за рубежом и признаваемую в Российской Федерации) и (или) учёное звание (в том числе учёное звание, полученное за рубежом и признаваемое в Российской Федерации), в общем числе научно-педагогических работников, реализующих программу специалитета, должна быть не менее 75 процентов.

К научно-педагогическим работникам с учёными степенями и (или) учёными званиями приравняются преподаватели Модуля военной подготовки без учёных степеней и (или) учёных званий, имеющие профильное высшее образование, опыт военной службы в области и с объектами профессиональной деятельности, соответствующими программе специалитета, не менее 10 лет, воинское (специальное) звание не ниже «майор» («капитан 3 ранга»), а также имеющие боевой опыт, или государственные награды, или государственные (отраслевые) почетные звания, или государственные премии.

6.2.4. Доля работников (в приведенных к целочисленным значениям ставок) из числа руководителей и работников организаций, деятельность которых связана с направленностью (профилем) реализуемой программы специалитета (имеющих стаж работы в данной профессиональной области не менее 3 лет), в общем числе работников, реализующих программу специалитета, должна быть не менее 10 процентов.

6.2.5. Все научно-педагогические работники, привлекаемые к реализации ОПОП, должны проходить повышение квалификации или стажировки не реже одного раза в три года, направленные на повышение компетенций в области преподавания, активных методов обучения, методов оценки результатов обучения. Научно-педагогические работники, участвующие в реализации профессиональных дисциплин и руководстве проектной деятельностью, должны проходить повышение квалификации или стажировку на профильных предприятиях, направленные на формирование у них личностных и межличностных навыков, навыков создания продуктов и систем.

6.3. Требования к материально-техническому и учебно-методическому обеспечению программы специалитета.

6.3.1. Специальные помещения должны представлять собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ, творческих проектов), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Специальные

помещения должны быть укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Перечень материально-технического обеспечения, необходимого для реализации программы специалитета, включает в себя лаборатории, оснащённые лабораторным оборудованием, в зависимости от степени сложности. Конкретные требования к материально-техническому и учебно-методическому обеспечению определяются образовательной программой.

ЮФУ обеспечивает наличие для студентов специальности рабочих пространств для инженерной деятельности и лабораторий, которые поддерживают и способствуют практическому освоению методов создания продуктов, процессов, систем, получению дисциплинарных знаний и изучению социальных аспектов.

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ЮФУ.

В случае применения электронного обучения, дистанционных образовательных технологий допускается замена специально оборудованных помещений их виртуальными аналогами, позволяющими обучающимся осваивать умения и навыки, предусмотренные профессиональной деятельностью.

6.3.2. В случае отсутствия требуемых изданий в электронно-библиотечной системе (электронной библиотеке) ЮФУ библиотечный фонд должен быть укомплектован печатными изданиями из расчета не менее 50 экземпляров каждого из изданий основной литературы, перечисленной в рабочих программах дисциплин (модулей), практик, и не менее 25 экземпляров дополнительной литературы на 100 обучающихся.

6.3.3. ЮФУ обеспечивает учебный процесс необходимым комплектом лицензионного программного обеспечения (состав определяется в рабочих программах дисциплин (модулей) и подлежит ежегодному обновлению).

6.3.4. Электронно-библиотечные системы (электронная библиотека) и электронная информационно-образовательная среда должны обеспечивать одновременный доступ не менее 25 процентов обучающихся по программе специалитета.

6.3.5. Обучающимся должен быть обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и подлежит ежегодному обновлению.

6.3.6. Обучающиеся из числа лиц с ограниченными возможностями здоровья должны быть обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

6.4. Требования к финансовым условиям реализации программы специалитета.

6.4.1. Финансовое обеспечение реализации программы должно осуществляться в объёме не ниже установленных Министерством образования и науки Российской Федерации базовых нормативных затрат на оказание государственной услуги в сфере образования для данного уровня образования и направления подготовки с учётом корректирующих коэффициентов, учитывающих специфику образовательных программ.

ПРИЛОЖЕНИЕ № 1

к образовательному стандарту

Южного федерального университета,

утвержденному приказом

от «24» ноября 2017 г. № 229-ОД

**Перечень профессиональных стандартов (далее – ПС),
соответствующих профессиональной деятельности выпускников программ
специалитета по специальности 10.05.02 Информационная безопасность
телекоммуникационных систем**

№ п/п	Наименование профессионального стандарта	Приказ Минтруда России		Регистрационный номер Минюста России	
		номер	дата	номер	дата
06 Связь, информационные и коммуникационные технологии					
1	Специалист по защите информации в телекоммуникационных системах и сетях	608н	03.11.2016	44449	25.11.2016
2	Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности	611н	09.11.2016	44398	22.11.2016
3	Специалист по безопасности компьютерных систем и сетей	598н	01.11.2016	44464	28.11.2016
4	Специалист по защите информации в	522н	15.09.2016	43857	28.09.2016

	автоматизированных системах				
5	Специалист по технической защите информации	599н	01.11.2016	44443	25.11.2016
6	Специалист по радиосвязи и телекоммуникациям	318н	19.05.2014	32595	05.06.2014
7	Инженер-проектировщик в области связи (телекоммуникаций)	316н	19.05.2014	33047	10.07.2014
8	Инженер связи (телекоммуникаций)	866н	31.10.2014	34971	28.11.2014
9	Оператор связи	275н	06.07.2015	37408	28.07.2015
10	Специалист по администрированию сетевых устройств информационно-коммуникационных систем	686н	05.10.2015	39568	30.10.2015
12 Обеспечение безопасности					
11	Специалист по противодействию иностранным техническим разведкам	831н			
40 Сквозные виды профессиональной деятельности					
12	Специалист по научно-исследовательским и опытно-конструкторским работам	121н	04.03.2014	31692	21.03.2014

ПРИЛОЖЕНИЕ № 2

к образовательному стандарту

Южного федерального университета,

утвержденному приказом

от «24» июля 2017 г. № 229-ОД

**Соответствие компетенций, установленных федеральным
государственным образовательным стандартом* и образовательным
стандартом ЮФУ по направлению специальности 10.05.02 Информационная
безопасность телекоммуникационных систем**

ФГОС ВО*	ОС ЮФУ
общекультурные	
способность использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1)	способность использовать социально-гуманитарные знания, культуру мышления, системный подход и критический анализ при формировании мировоззренческой и гражданской позиции (УК-1)
способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);	способность использовать экономические и правовые знания в профессиональной и социальной деятельности (УК-5)
способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3)	способность использовать социально-гуманитарные знания, культуру мышления, системный подход и критический анализ при формировании мировоззренческой и гражданской позиции (УК-1)
способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4)	способность использовать экономические и правовые знания в профессиональной и социальной деятельности (УК-5)
способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты	способность использовать социально-гуманитарные знания, культуру мышления, системный подход и критический анализ при формировании мировоззренческой и гражданской позиции (УК-1)

интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5)	
способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6)	способностью работать в команде, принимать организационно-управленческие решения и готовность нести за них ответственность (УК-3)
способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7)	способностью аргументированно, логически верно и содержательно строить устную и письменную речь, демонстрируя личную и профессиональную культуру, владеть русским и иностранным языками для решения коммуникативных задач во всех сферах общения (УК-2)
способностью к самоорганизации и самообразованию (ОК-8)	способностью к саморазвитию и самосовершенствованию, проявлению творческого подхода, готовности к повышению своей квалификации и мастерства (УК-4)
способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9)	способностью поддерживать уровень физической подготовки для обеспечения полноценной социальной и профессиональной деятельности, создавать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций (УК-7)
общепрофессиональные	
способностью анализировать физические явления и процессы для формализации и решения задач, возникающих в ходе профессиональной деятельности (ОПК-1)	способностью применять междисциплинарные знания для решения профессиональных задач с учётом смежных областей науки и практики (ОПК-1) способностью понимать естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять общенаучные методы при

	решении инженерных задач (ОПК-4)
способность применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)	способность понимать естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять общенаучные методы при решении инженерных задач (ОПК-4)
способность применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач (ОПК-3)	способность эффективно применять технические и программные средства и технологии в профессиональной деятельности (ОПК-5) способность применять положения теорий радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач (ОПК-9)
способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации (ОПК-4)	способность решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);
способность применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач (ОПК-5)	способность эффективно применять технические и программные средства и технологии в профессиональной деятельности (ОПК-5) владеть навыками установки, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ОПК-7)
способность применять методы научных исследований в профессиональной деятельности (ОПК-6)	способность понимать естественнонаучную сущность проблем, возникающих в ходе

	<p>профессиональной деятельности, и применять общенаучные методы при решении инженерных задач (ОПК-4)</p> <p>способность осуществлять проектную деятельность в профессиональной сфере (ОПК-2)</p>
<p>способность применять нормативные правовые акты в своей профессиональной деятельности (ОПК-7)</p>	<p>способность использовать экономические и правовые знания в профессиональной и социальной деятельности (УК-5)</p> <p>способность управлять информационной безопасностью объекта защиты (ОПК-8)</p>
<p>способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-8)</p>	<p>способность поддерживать уровень физической подготовки для обеспечения полноценной социальной и профессиональной деятельности, создавать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций (УК-7)</p>
профессиональные	
<p>способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1)</p>	<p>способность решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3)</p>
<p>способность формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов (ПК-2)</p>	<p>способность формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов (ПК-1)</p>
<p>способность оценивать технические</p>	<p>способность оценивать технические</p>

возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств (ПК-3)	возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств (ПК-2)
способность участвовать в разработке компонентов телекоммуникационных систем (ПК-4)	способность разрабатывать компоненты телекоммуникационных систем (ПК-3)
способность проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов (ПК-5)	способность проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания (ПК-4) способность разрабатывать проектную и отчётную документацию, представлять результаты профессиональной деятельности (ОПК-6)
способность применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-6)	способность применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-5)
способность осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования (ПК-7)	способность осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования (ПК-6)
способность проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем (ПК-8)	способность проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем (ПК-7)
способность участвовать в проведении аттестации телекоммуникационных систем	способность проводить аттестацию телекоммуникационных систем по

систем по требованиям защиты информации (ПК-9)	требованиям защиты информации (ПК-8)
способность оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений (ПК-10)	способность оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений (ПК-9)
способность организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы (ПК-11)	способность организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы (ПК-10)
способность выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности (ПК-12)	способность выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности (ПК-11)
способность организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем (ПК-13)	способность организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем (ПК-12)
способность выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты	способность выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты

телекоммуникационных сетей и систем (ПК-14)	телекоммуникационных сетей и систем (ПК-13)
способность проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания (ПК-15)	способность проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания (ПК-14)
профессионально-специализированные	
способность разрабатывать алгоритмы преобразования информации и сигналов для защищенных телекоммуникационных систем на основе теоретико-числовых методов (ПСК-7.1);	способность разрабатывать алгоритмы преобразования информации и сигналов для защищенных телекоммуникационных систем на основе теоретико-числовых методов (ПСК-1.1);
способность выбирать методы и разрабатывать алгоритмы принятия решений в защищенных телекоммуникационных системах (ПСК-7.2);	способность выбирать методы и разрабатывать алгоритмы принятия решений в защищенных телекоммуникационных системах (ПСК-1.2);
способность разрабатывать аппаратное и программное обеспечение узлов и устройств защищенных телекоммуникационных систем на базе сигнальных процессоров (ПСК-7.3);	способность разрабатывать аппаратное и программное обеспечение узлов и устройств защищенных телекоммуникационных систем на базе сигнальных процессоров (ПСК-1.3);
способность участвовать в разработке систем управления информационной безопасностью телекоммуникационных систем (ПСК-7.4);	способность разрабатывать системы управления информационной безопасностью телекоммуникационных систем (ПСК-1.4);
способность обеспечивать защиту программных средств защищенных телекоммуникационных систем (ПСК-7.5);	способность обеспечивать защиту программных средств защищенных телекоммуникационных систем (ПСК-1.5);
способность выбирать методы и разрабатывать алгоритмы для обеспечения безопасности СПЦЗС (ПСК-8.1);	способность выбирать методы и разрабатывать алгоритмы для обеспечения безопасности СПЦЗС (ПСК-2.1);
способность использовать и реализовать современные алгоритмы обработки информации и сигналов в целях	способность использовать и реализовать современные алгоритмы обработки информации и сигналов в

обеспечения безопасности СПЦЗС (ПСК-8.2);	целях обеспечения безопасности СПЦЗС (ПСК-2.2);
способность модифицировать аппаратное и программное обеспечение узлов и устройств СПЦЗС (ПСК-8.3);	способность модифицировать аппаратное и программное обеспечение узлов и устройств СПЦЗС (ПСК-2.3);
способность контролировать работоспособность и определять эффективность средств защиты информации в СПЦЗС (ПСК-8.4);	способность контролировать работоспособность и определять эффективность средств защиты информации в СПЦЗС (ПСК-2.4);
способность разрабатывать узлы и устройства, минимизирующие информационные риски и увеличивающие живучесть СПЦЗС (ПСК-8.5);	способность разрабатывать узлы и устройства, минимизирующие информационные риски и увеличивающие живучесть СПЦЗС (ПСК-2.5);
способность использовать нормативные правовые акты и нормативные методические документы в области технологий и систем радиосвязи и телерадиовещания (ПСК-9.1);	способность использовать нормативные правовые акты и нормативные методические документы в области технологий и систем радиосвязи и телерадиовещания (ПСК-3.1);
способность участвовать в процедурах назначения, распределения и эффективного использования радиочастотного спектра (ПСК-9.2);	владеть процедурами назначения, распределения и эффективного использования радиочастотного спектра (ПСК-3.2);
способность применять методы повышения помехоустойчивости и защищенности систем радиосвязи и телерадиовещания и определять эффективность их использования (ПСК-9.3);	способность применять методы повышения помехоустойчивости и защищенности систем радиосвязи и телерадиовещания и определять эффективность их использования (ПСК-3.3);
способность проводить измерения основных характеристик и параметров телекоммуникационных систем с целью оценки их соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов (ПСК-9.4);	способность проводить измерения основных характеристик и параметров телекоммуникационных систем с целью оценки их соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов (ПСК-3.4);
способность разрабатывать системы, сети и устройства защищенной радиосвязи и	способность разрабатывать системы, сети и устройства защищенной

телерадиовещания (ПСК-9.5);	радиосвязи и телерадиовещания (ПСК-3.5);
способность применять теорию сигналов и систем для анализа телекоммуникационных систем и оценки их помехоустойчивости (ПСК-10.1);	способность применять теорию сигналов и систем для анализа телекоммуникационных систем и оценки их помехоустойчивости (ПСК-4.1);
способность формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем (ПСК-10.2);	способность формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем (ПСК-4.2);
способность оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации (ПСК-10.3);	способность оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации (ПСК-4.3);
способность применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации (ПСК-10.4);	способность применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации (ПСК-4.4);
способность проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи (ПСК-10.5);	способность проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи (ПСК-4.5);
способность проводить теоретические и экспериментальные исследования телекоммуникационных систем и сетей транспорта (по видам) и оценивать их эффективность (ПСК-11.1);	способность проводить теоретические и экспериментальные исследования телекоммуникационных систем и сетей транспорта (по видам) и оценивать их эффективность (ПСК-5.1);
способность осуществлять рациональный выбор методов и средств обеспечения информационной безопасности телекоммуникационных систем и сетей транспорта (по видам) (ПСК-11.2);	способность осуществлять рациональный выбор методов и средств обеспечения информационной безопасности телекоммуникационных систем и сетей транспорта (по видам)

	(ПСК-5.2);
способность разрабатывать предложения по совершенствованию системы аудита и управления информационной безопасностью телекоммуникационных систем и сетей транспорта (по видам) (ПСК-11.3);	способность разрабатывать предложения по совершенствованию системы аудита и управления информационной безопасностью телекоммуникационных систем и сетей транспорта (по видам) (ПСК-5.3);
способность к профессиональной эксплуатации современного оборудования, использовать методы и средства измерений для решения метрологических задач и технической диагностики защищенных систем и сетей транспорта (по видам) (ПСК-11.4);	способность к профессиональной эксплуатации современного оборудования, использовать методы и средства измерений для решения метрологических задач и технической диагностики защищенных систем и сетей транспорта (по видам) (ПСК-5.4);
способность обеспечить эффективную защиту телекоммуникационных систем и сетей транспорта (по видам) (ПСК-11.5);	способность обеспечить эффективную защиту телекоммуникационных систем и сетей транспорта (по видам) (ПСК-5.5);
способность выполнять декомпозицию сложных информационных систем, формулировать показатели их эффективности с целью построения корректной концептуальной модели систем (ПСК-12.1);	способность выполнять декомпозицию сложных информационных систем, формулировать показатели их эффективности с целью построения корректной концептуальной модели систем (ПСК-6.1);
способность обоснованно выбирать и (или) строить адекватные, математические и алгоритмические модели, в том числе с помощью высокоуровневых средств, для эффективного проектирования телекоммуникационных систем информационного взаимодействия (ПСК-12.2);	способность обоснованно выбирать и (или) строить адекватные, математические и алгоритмические модели, в том числе с помощью высокоуровневых средств, для эффективного проектирования телекоммуникационных систем информационного взаимодействия (ПСК-6.2);
способность обоснованно выбирать и применять адекватные методы кодирования для построения высокоэффективных телекоммуникационных систем информационного взаимодействия и	способность обоснованно выбирать и применять адекватные методы кодирования для построения высокоэффективных телекоммуникационных систем информационного взаимодействия и

систем управления их поведением (ПСК-12.3);	систем управления их поведением (ПСК-6.3);
способность анализировать информационные потоки на пакетном уровне, оценивать реальный уровень безопасности информационного взаимодействия и предлагать эффективные меры для его повышения (ПСК-12.4);	способность анализировать информационные потоки на пакетном уровне, оценивать реальный уровень безопасности информационного взаимодействия и предлагать эффективные меры для его повышения (ПСК-6.4);
способность применять стандартные средства для анализа программного кода с целью оценки уровня его защиты от исследования и поиска несанкционированного или вредоносного вмешательства в работу телекоммуникационных систем информационного взаимодействия (ПСК-12.5).	способность применять стандартные средства для анализа программного кода с целью оценки уровня его защиты от исследования и поиска несанкционированного или вредоносного вмешательства в работу телекоммуникационных систем информационного взаимодействия (ПСК-6.5).
	способностью понимать и нести ответственность за принимаемые решения и проектируемые объекты профессиональной деятельности в социально-экономическом контексте инженерной деятельности (ПК-15)
	способностью разрабатывать бизнес-планы предприятий профессиональной сферы, осуществлять мероприятия по созданию предприятий, по организации и управлению их работой (ПК-16)
	способностью управлять капитализацией компании и её финансами, осуществлять маркетинг инновационной продукции на рынке продуктов и услуг в области информационной безопасности телекоммуникационных систем (ПК-17)
	способностью осуществлять планирование производства продукции и (или) услуг с использованием

	инновационных технологий (ПК-18)
	способностью формировать команды и разрабатывать системы стимулирования инженерных процессов (ПК-19)
	способностью осуществлять управление интеллектуальной собственностью (ПК-20)

*Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по специальности 10.05.02 Информационная безопасность телекоммуникационных систем (квалификация (степень) «специалист»), утверждённый приказом Министерства образования и науки Российской Федерации от «16» ноября 2016 г. № 1426.