МИНОБРНАУКИ РОССИИ

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

ПРИКАЗ

«26» мая 2017 г. № 187-ОД

г. Ростов-на-Дону

Об утверждении образовательного стандарта Южного федерального университета по специальности 10.05.03 Информационная безопасность автоматизированных систем

На основании решения Ученого совета ЮФУ от 26 мая 2017 года (Протокол № 5) п р и к а з ы в а ю:

1. Утвердить прилагаемый образовательный стандарт Южного федерального университета по специальности 10.05.03 Информационная безопасность автоматизированных систем.

2. Структурным подразделениям, реализующим образовательные программы по специальности 10.05.03 Информационная безопасность автоматизированных 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 специальности 10.05.03 Информационная безопасность автоматизированных 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.

И.о. ректора М.А. Боровская

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Утверждён приказом Южного федерального университета от «26» января 2017 г. №187-ОД

Принят Учёным советом ЮФУ «26» мая 2017 г. Протокол № 5

ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ОБРАЗОВАНИЯ ЮЖНОГО ФЕДЕРАЛЬНОГО УНИВЕРСИТЕТА

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность

10.05.03 Информационная безопасность автоматизированных 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 10.05.03 Информационная безопасность автоматизированных 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 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утверждённый приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. № 1509;
- Профессиональные стандарты (Приложение № 1);
- Всемирная инициатива CDIO. Стандарты;
- Всемирная инициатива CDIO. Планируемые результаты обучения (CDIO Syllabus);
- 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.

Объём программы специалитета составляет 300 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 лет. Объём программы специалитета в очной форме обучения, реализуемый за один учебный год, составляет 60 з.е.;

при обучении по индивидуальному учебному плану вне зависимости от формы обучения устанавливается ЮФУ самостоятельно, 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. Объём 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 автоматизированных систем в условиях существования угроз в информационной сфере.

3.2. Объектами профессиональной деятельности выпускников, освоивших программу специалитета, являются: автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем; системы управления информационной безопасностью автоматизированных систем.

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

– **научно-исследовательская;**

– **проектно-конструкторская;**

– **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 «Информационная безопасность автоматизированных систем критически важных объектов»;

специализация №2 «Безопасность открытых информационных систем»;

специализация №3 «Информационная безопасность автоматизированных банковских систем»;

специализация №4 «Защищённые автоматизированные системы управления»;

специализация №5 «Обеспечение информационной безопасности распределённых информационных систем»;

специализация №6 «Анализ безопасности информационных систем»;

специализация №7 «Создание автоматизированных систем в защищённом исполнении»;

специализация №8 «Информационная безопасность автоматизированных систем на транспорте».

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 по проблематике информационной безопасности автоматизированных систем;

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

моделирование и исследование свойств защищенных автоматизированных систем;

анализ защищённости информации в автоматизированных системах и безопасности реализуемых информационных технологий;

разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;

– **проектно-конструкторская деятельность:**

сбор и анализ исходных данных для проектирования защищённых автоматизированных систем;

разработка политик информационной безопасности автоматизированных систем;

разработка защищённых автоматизированных систем в сфере профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;

выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищённых автоматизированных систем;

разработка систем управления информационной безопасностью автоматизированных систем;

– **контрольно-аналитическая:**

контроль работоспособности и эффективности применяемых средств защиты информации;

выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;

проведение инструментального мониторинга защищённости автоматизированных систем и анализа его результатов;

- **организационно-управленческая деятельность:**

организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;

организационно-методическое обеспечение информационной безопасности автоматизированных систем;

организация работ по созданию, внедрению, эксплуатации и сопровождению защищённых автоматизированных систем;

контроль реализации политики информационной безопасности;

- **эксплуатационная деятельность:**

реализация информационных технологий в сфере профессиональной деятельности с использованием защищённых автоматизированных систем;

администрирование подсистем информационной безопасности автоматизированных систем;

мониторинг информационной безопасности автоматизированных систем;

управление информационной безопасностью автоматизированных систем;

обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;

- **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 специализацией программы специалитета:**

специализация №1 «Информационная безопасность автоматизированных систем критически важных объектов»:

оценка эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов;

разработка, внедрение и эксплуатация средств защиты информации, включая системы их мониторинга, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов;

разработка технических регламентов для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов;

специализация №2 «Безопасность открытых информационных систем»:

разработка и реализация политики информационной безопасности открытых информационных систем;

проектирование, эксплуатация и совершенствование системы управления информационной безопасностью открытой информационной системы;

контроль обеспечения информационной безопасности открытой информационной системы;

специализация №3 «Информационная безопасность автоматизированных банковских систем»:

разработка и реализация политики информационной безопасности автоматизированных банковских систем;

проектирование, эксплуатация и совершенствование системы управления информационной безопасностью автоматизированных банковских систем;

контроль обеспечения информационной безопасности автоматизированных банковских систем;

специализация №4 «Защищённые автоматизированные системы управления»:

выявление режимов работы элементов защищённых автоматизированных систем управления и внешних воздействий на них, способствующих увеличению риска утечки информации в различных физических полях;

разработка защищённых автоматизированных систем управления, в том числе подсистем мониторинга их информационной безопасности;

планирование, реализация, оценка и коррекция основных процессов управления информационной безопасностью защищённых автоматизированных систем управления и организаций;

специализация №5 «Обеспечение информационной безопасности распределённых информационных систем»:

разработка и исследование моделей информационно-технологических ресурсов, модели угроз и модели нарушителей информационной безопасности в распределеённых информационных системах;

удаленное администрирование операционных систем и систем баз данных в распределённых информационных системах;

аудит защищённости информационно-технологических ресурсов;

координация деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятиях и в учреждениях;

специализация №6 «Анализ безопасности информационных систем»:

использование языков, систем, инструментальных программных и аппаратных средства для моделирования информационных систем и испытаний систем защиты, в том числе анализа безопасности программного обеспечения;

разработка модели угроз и модели нарушителя информационной безопасности, методик и тестов для анализа степени защищённости информационной системы и её соответствия нормативным требованиям по защите информации;

участие в сертификационных испытаниях по существующим требованиям;

специализация №7 «Создание автоматизированных систем в защищённом исполнении»:

моделирование, разработка, реализация и управление процессами создания и эксплуатации автоматизированных систем в защищённом исполнении на всех стадиях и этапах их жизненного цикла;

анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищённом исполнении;

специализация №8 «Информационная безопасность автоматизированных систем на транспорте»:

разработка защищённых автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с использованием программных, программно-аппаратных и технических методов и средств защиты информации;

разработка политики безопасности для совершенствования системы управления информационной безопасностью распределённых автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам);

мониторинг и аудит уровня защищённости, оценка соответствия и аттестация распределённых автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учётом нормативных документов по защите информации.

IV. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4.1. В результате освоения программы специалитета у выпускника должны быть сформированы универсальные, общепрофессиональные, профессиональные, профессионально-специализированные компетенции. Соответствие компетенций, установленных федеральным государственным образовательным стандартом и образовательным стандартом ЮФУ по специальности 10.05.03 Информационная

безопасность автоматизированных 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);

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

способностью к саморазвитию и самосовершенствованию, проявлению творческого подхода, готовность 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 по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ОПК-7);

способностью управлять информационной безопасностью объекта защиты (ОПК-8).

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

научно-исследовательская деятельность:

способностью создавать и исследовать модели автоматизированных систем, модели угроз и модели нарушителя с целью анализа уязвимостей и разработки эффективных решений по обеспечению информационной безопасности автоматизированных систем (ПК-1);

способностью проводить анализ защищённости и анализ рисков информационной безопасности автоматизированных систем (ПК-2);

способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере

профессиональной деятельности (ПК-3);

проектно-конструкторская деятельность:

способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем, систем управления и средств управления информационной безопасностью (ПК-4);

способностью разрабатывать защищённые автоматизированные системы в сфере профессиональной деятельности (ПК-5);

способностью формулировать требования и проектировать, разрабатывать и тестировать программно-аппаратные средства защиты информации компьютерных систем, сетей, систем управления информационной безопасностью (ПК -6);

способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-7);

контрольно-аналитическая деятельность:

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-8);

владеть навыками проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-9);

владеть навыками проведения экспериментально-исследовательских работ при аттестации автоматизированных систем с учётом нормативных документов по защите информации (ПК-10);

способностью проводить инструментальный мониторинг защищённости информации в автоматизированной системе и выявлять каналы утечки информации (ПК-11);

организационно-управленческая деятельность:

способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере

профессиональной деятельности (ПК-12);

способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учётом требований информационной безопасности (ПК-13);

способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, и предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-14);

владеть процедурами формирования политики информационной безопасности организации и контролировать эффективность её реализации (ПК-15);

способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-16);

эксплуатационная деятельность:

способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности, разрабатывать и обеспечивать восстановление их работоспособности при возникновении нештатных ситуаций (ПК-17);

способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-18);

способностью выполнять полный объём работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-19).

инженерно-предпринимательская деятельность:

способностью понимать и нести ответственность за принимаемые решения и проектируемые объекты профессиональной деятельности в социально-экономическом контексте инженерной деятельности (ПК-20);

способностью разрабатывать бизнес-планы предприятий профессиональной сферы, осуществлять мероприятия по созданию предприятий, по организации и управлению их работой (ПК-21);

способностью управлять капитализацией компании и её финансами, осуществлять маркетинг инновационной продукции на рынке продуктов и услуг в области информационной безопасности автоматизированных систем (ПК-22);

способностью осуществлять планирование производства продукции и (или) услуг с использованием инновационных технологий (ПК-23);

способностью формировать команды и разрабатывать системы стимулирования инженерных процессов (ПК-24);

способностью осуществлять управление интеллектуальной собственностью (ПК-25).

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

специализация №1 «Информационная безопасность автоматизированных систем критически важных объектов»:

способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-1.1);

способностью разрабатывать, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-1.2);

способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов (ПСК-1.3);

способностью разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных

объектов и автоматизированных систем критически важных объектов (ПСК-1.4);

способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-1.5);

специализация №2 «Безопасность открытых информационных систем»:

способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-2.1);

способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-2.2);

способностью проектирования, эксплуатации и совершенствованию системы управления информационной безопасностью открытой информационной системы (ПСК-2.3);

способностью организовывать и проводить контроль обеспечения информационной безопасности открытой информационной системы (ПСК-2.4);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приёмы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-2.5);

специализация №3 «Информационная безопасность автоматизированных банковских систем»:

способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем (ПСК-3.1);

способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем (ПСК-3.2);

способностью проектировать, обслуживать и совершенствовать системы управления информационной безопасностью автоматизированных банковских

систем (ПСК-3.3);

способностью организовывать и проводить контроль обеспечения информационной безопасности автоматизированных банковских систем (ПСК-3.4);

способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы (ПСК-3.5);

специализация №4 «Защищённые автоматизированные системы управления»:

способностью выявлять режимы работы элементов защищённых автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях (ПСК-4.1);

способностью разрабатывать подсистемы мониторинга информационной безопасности защищённых автоматизированных систем управления (ПСК-4.2);

способностью планировать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью защищённых автоматизированных систем управления и организаций (ПСК-4.3);

способностью разрабатывать защищённые автоматизированные системы управления, применять современные технологии их проектирования (ПСК-4.4);

способностью разрабатывать и оценивать соответствие средств защиты информации подсистем обеспечения информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации (ПСК-4.5);

специализация №5 «Обеспечение информационной безопасности распределённых информационных систем»:

способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя

информационной безопасности в распределённых информационных системах (ПСК-5.1);

способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределённых информационных системах (ПСК-5.2);

способностью проводить аудит защищённости информационно-технологических ресурсов распределённых информационных систем (ПСК-5.3);

способностью проводить удаленное администрирование операционных систем и систем баз данных в распределённых информационных системах (ПСК-5.4);

способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-5.5);

специализация №6 «Анализ безопасности информационных систем»:

способностью использовать языки, системы, инструментальные программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты (ПСК-6.1);

способностью разрабатывать методики и тесты для анализа степени защищённости информационной системы, соответствия нормативным требованиям по защите информации (ПСК-6.2);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности, планировать объём тестовых проверок (ПСК-6.3);

способностью применять инструментарий анализа безопасности программного обеспечения (ПСК-6.4);

способностью проведения сертификационных испытаний по существующим требованиям (ПСК-6.5);

специализация №7 «Создание автоматизированных систем в защищённом исполнении»:

способностью моделирования, разработки, реализации и управления

процессами создания и эксплуатации автоматизированных систем в защищённом исполнении на всех стадиях и этапах их жизненного цикла (ПСК-7.1);

способностью рационально выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищённом исполнении (ПСК-7.2);

способностью применять современные технологии проектирования автоматизированных систем в защищённом исполнении (ПСК-7.3);

способностью применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищённом исполнении на различных стадиях их жизненного цикла (ПСК-7.4);

способностью проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищённом исполнении (ПСК-7.5);

специализация №8 «Информационная безопасность автоматизированных систем на транспорте»:

способностью разрабатывать защищённые автоматизированные, информационно-управляющие и информационно-логистические системы на транспорте (по видам) с использованием программных, программно-аппаратных и технических методов и средств защиты информации (ПСК-8.1);

способностью разрабатывать политику безопасности для совершенствования системы управления информационной безопасностью распределённых автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-8.2);

способностью осуществлять рациональный выбор средств и разрабатывать предложения по обеспечению информационной безопасности распределённых автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-8.3);

способностью осуществлять мониторинг и аудит уровня защищённости,

оценку соответствия и аттестацию распределённых автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учётом нормативных требований по защите информации (ПСК-8.4);

способностью обеспечить эффективное применение средств защиты электронного технологического документооборота и технического документоведения на транспорте (по видам) (ПСК-8.5).

4.6. При разработке программы специалитета все универсальные, общепрофессиональные, профессиональные компетенции, отнесенные к тем видам профессиональной деятельности, на которые ориентирована программа специалитета, и профессионально-специализированные компетенции, отнесенные 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, 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 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)**	**261-267**
	Базовая часть, в том числе дисциплины (модули) специализации	186-216
	Вариативная часть	51-75
Блок 2	**Практики, в том числе научно-исследовательская работа (НИР)**	**27-30**
	Вариативная часть	27-30
Блок 3	**Государственная итоговая аттестация**	**6-9**
	Базовая часть	6-9
Объём программы специалитета		**300**

5.3. Дисциплины (модули), относящиеся к базовой части программы специалитета, являются обязательными для освоения обучающимся с учётом специализации программы, которую он осваивает. Набор дисциплин (модулей), относящихся к базовой части программы специалитета, руководитель направления подготовки определяет 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; стандартам и оформлению инженерной документации 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);
- элективными дисциплинами в объеме 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 учётом специализации программы, выбранных видов профессиональной деятельности в объёме, установленном настоящим стандартом. После выбора обучающимся специализации программы, набор соответствующих выбранной направленности дисциплин (модулей) становится обязательным для освоения обучающимся.

Трудоемкость всех дисциплин, кроме указанных в модуле общеуниверситетских дисциплин, модуле проектной деятельности и модуле военной подготовки, должны быть трудоёмкостью 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 и навыков.

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 разработчики выбирают типы практик в зависимости от видов деятельности, на которые ориентирована программа. Разработчики программы вправе предусмотреть иные типы практик дополнительно к установленным настоящим стандартом.

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.

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

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

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 партнерства, 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 применяемыми образовательными технологиями.

6.1.3. Для реализации компетентностного 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 приведённых 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 приведённых 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 приведённых к целочисленным значениям ставок) должно составлять не менее 5 в журналах, индексируемых в базах данных Web of Science или Scopus, или не менее 30 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 10.05.03 Информационная безопасность автоматизированных 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 и (или) учёную степень, соответствующие 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 70 процентов.

К научно-педагогическим работникам с учёными степенями и (или) учёными званиями приравниваются 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 приведённых 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 обучении, 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 организации.

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 (удалённый 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,
утверждённому приказом
от «26» июня 2017 г. № 187-ОД

УТВЕРЖДАЮ

И.о. ректора _____ М.А. Боровская

Перечень профессиональных стандартов (далее – ПС), соответствующих профессиональной деятельности выпускников программ специалитета по специальности 10.05.03 Информационная безопасность автоматизированных 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 автоматизированных системах	522н	15.09.2016	43857	28.09.2016
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,
утверждённому приказом
от «26» июня 2017 г. № 187-ОД

УТВЕРЖДАЮ
И.о. ректора М.А. Боровская

Соответствие компетенций, установленных федеральным государственным образовательным стандартом* и образовательным стандартом ЮФУ по направлению специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета)

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)
способность 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, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3)	способность соблюдать принципы и нормы толерантного отношения к носителям разных этнокультурных традиций, религиозных и политических взглядов в многонациональном и поликонфессиональном обществе (УК-6)
способность 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	способность к саморазвитию и самосовершенствованию, проявлению творческого подхода, готовность к повышению своей квалификации и мастерства (УК-4)

ФГОС ВО*	ОС ЮФУ
области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5)	
способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6)	способность работать в команде, принимать организационно-управленческие решения и готовность нести за них ответственность (УК-3)
способность 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)	способность 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)
способность к самоорганизации и самообразованию (ОК-8)	способность к саморазвитию и самосовершенствованию, проявлению творческого подхода, готовность к повышению своей квалификации и мастерства (УК-4)
способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9)	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)
общепрофессиональные	
способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1)	способность применять междисциплинарные знания для решения профессиональных задач с учётом смежных областей науки и практики (ОПК-1) способность понимать естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять общенаучные методы при решении

ФГОС ВО*	ОС ЮФУ
	инженерных задач (ОПК-4)
способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2)	способность решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности (ОПК-3) способность понимать естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять общенаучные методы при решении инженерных задач (ОПК-4)
способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3)	способность эффективно применять технические и программные средства и технологии в профессиональной деятельности (ОПК-5)
способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4)	способность осуществлять проектную деятельность в профессиональной сфере (ОПК-2) способность разрабатывать проектную и отчётную документацию, представлять результаты профессиональной деятельности (ОПК-6)
способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5)	способность понимать естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять общенаучные методы при решении инженерных задач (ОПК-4) способность осуществлять проектную деятельность в профессиональной сфере (ОПК-2) способность работать в команде, принимать организационно-управленческие решения и готовность нести за них ответственность (УК-3)
способность применять нормативные правовые акты в	способность использовать экономические и правовые знания в

ФГОС ВО*	ОС ЮФУ
профессиональной деятельности (ОПК-6)	профессиональной и социальной деятельности (УК-5) способность управлять информационной безопасностью объекта защиты (ОПК-8)
способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7)	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)
способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8)	способность осуществлять проектную деятельность в профессиональной сфере (ОПК-2) способность эффективно применять технические и программные средства и технологии в профессиональной деятельности (ОПК-5)
профессиональные	
способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1)	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 создавать и исследовать модели автоматизированных систем (ПК-2)	способность создавать и исследовать модели автоматизированных систем, модели угроз и модели нарушителя с целью анализа уязвимостей и разработки эффективных решений по обеспечению информационной безопасности автоматизированных систем (ПК-1)
способность проводить анализ защищенности автоматизированных систем (ПК-3)	способность проводить анализ защищенности и анализ рисков информационной безопасности автоматизированных систем (ПК-2)

ФГОС ВО*	ОС ЮФУ
способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4)	способность создавать и исследовать модели автоматизированных систем, модели угроз и модели нарушителя с целью анализа уязвимостей и разработки эффективных решений по обеспечению информационной безопасности автоматизированных систем (ПК-1)
способность проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5)	способность проводить анализ защищенности и анализ рисков информационной безопасности автоматизированных систем (ПК-2)
способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6)	способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-3)
способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7)	способность разрабатывать проектную и отчётную документацию, представлять результаты профессиональной деятельности (ОПК-6)
способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8)	способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем, систем управления и средств информационной безопасностью (ПК-4)
способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9)	способность разрабатывать защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-5) способность формулировать требования и проектировать, разрабатывать и тестировать программно-аппаратных средства защиты информации компьютерных систем и сетей и систем управления информационной безопасностью (ПК -6)
способность применять знания в	способность эффективно применять

ФГОС ВО*	ОС ЮФУ
области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10)	технические и программные средства и технологии в профессиональной деятельности (ОПК-5)
способность разрабатывать политику информационной безопасности автоматизированной системы (ПК-11)	способность разрабатывать политику информационной безопасности автоматизированной системы (ПК-7)
способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12)	способность управлять информационной безопасностью объекта защиты (ОПК-8) способность разрабатывать требования и способность формулировать требования и проектировать, разрабатывать и тестировать программно-аппаратных средства защиты информации компьютерных систем и сетей и систем управления информационной безопасностью (ПК - 6)
способность участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13)	способность формулировать требования и проектировать, разрабатывать и тестировать программно-аппаратных средства защиты информации компьютерных систем и сетей и систем управления информационной безопасностью (ПК -6)
способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14)	способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-8)
способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных	владеть навыками проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-9)

ФГОС ВО*	ОС ЮФУ
систем (ПК-15)	
способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16)	владеть навыками проведения экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-10)
способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17)	способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-11)
способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18)	способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-12)
способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19)	способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, и предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-14)
способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20)	способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-13)
способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21)	способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, и предложения по совершенствованию системы управления информационной

ФГОС ВО*	ОС ЮФУ
	безопасностью автоматизированной системы (ПК-14)
способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22)	владеть процедурами формирования политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-15)
способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23)	способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-16)
способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24)	способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности, разрабатывать и обеспечивать восстановление их работоспособности при возникновении нештатных ситуаций (ПК-17)
способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25)	способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности, разрабатывать и обеспечивать восстановление их работоспособности при возникновении нештатных ситуаций (ПК-17)
способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-26)	способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-18)
способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27)	способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-19)

ФГОС ВО*	ОС ЮФУ
способность управлять информационной безопасностью автоматизированной системы (ПК-28)	способность управлять информационной безопасностью объекта защиты (ОПК-8)
профессионально-специализированные	
способность проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-3.1);	способность проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-1.1);
способность участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-3.2);	способность разрабатывать, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов (ПСК-1.2);
способность применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов (ПСК-3.3);	способность применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов (ПСК-1.3);
способность разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов (ПСК-3.4);	способность разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов (ПСК-1.4);
способность проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах	способность проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах

ФГОС ВО*	ОС ЮФУ
критически важных объектов (ПСК-3.5);	критически важных объектов (ПСК-1.5);
способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1);	способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-2.1);
способность разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2);	способность разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-2.2);
способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3);	способность проектировать, обслуживать и совершенствовать системы управления информационной безопасностью открытой информационной системы (ПСК-2.3);
способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы (ПСК-4.4);	способность организации и проведения контроля обеспечения информационной безопасности открытой информационной системы (ПСК-2.4);
способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5);	способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-2.5);
способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем (ПСК-5.1);	способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем (ПСК-3.1);
способность разрабатывать и реализовывать политики	способность разрабатывать и реализовывать политики

ФГОС ВО*	ОС ЮФУ
информационной безопасности автоматизированных банковских систем (ПСК-5.2);	информационной безопасности автоматизированных банковских систем (ПСК-3.2);
способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью автоматизированных банковских систем (ПСК-5.3);	способность проектировать, обслуживать и совершенствовать системы управления информационной безопасностью автоматизированных банковских систем (ПСК-3.3);
способность участвовать в организации и проведении контроля обеспечения информационной безопасности автоматизированных банковских систем (ПСК-5.4);	способность организовывать и проводить контроль обеспечения информационной безопасности автоматизированных банковских систем (ПСК-3.4);
способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы (ПСК-5.5);	способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы (ПСК-3.5);
способность выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях (ПСК-6.1);	способность выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях (ПСК-4.1);
способность участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления (ПСК-6.2);	способность разрабатывать подсистемы мониторинга информационной безопасности защищенных автоматизированных систем управления (ПСК-4.2);
способность планировать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью защищенных автоматизированных систем управления и организаций (ПСК-6.3);	способность планировать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью защищенных автоматизированных систем управления и организаций (ПСК-4.3);

ФГОС ВО*	ОС ЮФУ
способность участвовать в разработке защищенных автоматизированных систем управления, применять современные технологии их проектирования (ПСК-6.4);	способность разрабатывать защищенные автоматизированные системы управления, применять современные технологии их проектирования (ПСК-4.4);
способность участвовать в разработке и оценке соответствия средств защиты информации подсистем обеспечения информационной безопасности защищенных автоматизированных систем управления нормативным требованиям по защите информации (ПСК-6.5);	способность разрабатывать и оценивать соответствие средств защиты информации подсистем обеспечения информационной безопасности защищенных автоматизированных систем управления нормативным требованиям по защите информации (ПСК-4.5);
способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);	способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-5.1);
способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);	способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-5.2);
способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);	способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-5.3);
способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4);	способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-5.4);
способность координировать деятельность подразделений и специалистов по защите	способность координировать деятельность подразделений и специалистов по защите информации в

ФГОС ВО*	ОС ЮФУ
информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5);	организациях, в том числе на предприятии и в учреждении (ПСК-5.5);
способность использовать языки, системы, инструментальные программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты (ПСК-8.1);	способность использовать языки, системы, инструментальные программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты (ПСК-6.1);
способность разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации (ПСК-8.2);	способность разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации (ПСК-6.2);
способность разрабатывать модели угроз и модели нарушителя информационной безопасности, планировать объем тестовых проверок (ПСК-8.3);	способность разрабатывать модели угроз и модели нарушителя информационной безопасности, планировать объем тестовых проверок (ПСК-6.3);
способность применять инструментарий анализа безопасности программного обеспечения (ПСК-8.4);	способность применять инструментарий анализа безопасности программного обеспечения (ПСК-6.4);
способность участвовать в сертификационных испытаниях по существующим требованиям (ПСК-8.5);	способность проведения сертификационных испытаний по существующим требованиям (ПСК-6.5);
способность принимать участие в моделировании, разработке, реализации и управлении процессами создания и эксплуатации автоматизированных систем в защищенном исполнении на всех стадиях и этапах их жизненного цикла (ПСК-9.1);	способность моделирования, разработки, реализации и управления процессами создания и эксплуатации автоматизированных систем в защищённом исполнении на всех стадиях и этапах их жизненного цикла (ПСК-7.1);
способность рационально выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в	способность рационально выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в

ФГОС ВО*	ОС ЮФУ
защищенном исполнении (ПСК-9.2);	защищенном исполнении (ПСК-7.2);
способность применять современные технологии проектирования автоматизированных систем в защищенном исполнении (ПСК-9.3);	способность применять современные технологии проектирования автоматизированных систем в защищенном исполнении (ПСК-7.3);
способность применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла (ПСК-9.4);	способность применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла (ПСК-7.4);
способность проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении (ПСК-9.5);	способность проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении (ПСК-7.5);
способность участвовать в разработке защищенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с использованием программных, программно-аппаратных и технических методов и средств защиты информации (ПСК-10.1);	способность разрабатывать защищённые автоматизированные, информационно-управляющие и информационно-логистические системы на транспорте (по видам) с использованием программных, программно-аппаратных и технических методов и средств защиты информации (ПСК-8.1);
способность разрабатывать политику безопасности для совершенствования системы управления информационной безопасностью распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-10.2);	способность разрабатывать политику безопасности для совершенствования системы управления информационной безопасностью распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-8.2);
способность осуществлять рациональный выбор средств и	способность осуществлять рациональный выбор средств и

ФГОС ВО*	ОС ЮФУ
разрабатывать предложения по обеспечению информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-10.3);	разрабатывать предложения по обеспечению информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-8.3);
способность осуществлять мониторинг и аудит уровня защищенности, оценку соответствия и аттестацию распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учетом нормативных требований по защите информации (ПСК-10.4);	способность осуществлять мониторинг и аудит уровня защищенности, оценку соответствия и аттестацию распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учетом нормативных требований по защите информации (ПСК-8.4);
способность обеспечить эффективное применение средств защиты электронного технологического документооборота и технического документоведения на транспорте (по видам) (ПСК-10.5).	способность обеспечить эффективное применение средств защиты электронного технологического документооборота и технического документоведения на транспорте (по видам) (ПСК-8.5).

* федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утверждённый приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. № 1509.